(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－67256
（P2003－67256A）
(43)公開日　平成15年３月７日(2003.3.7)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｆ	５Ｂ０１７
3/06	３０４	3/06	３０４Ｍ	５Ｂ０６５
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ａ	５Ｊ１０４
			６０１Ｅ	

審査請求　未請求　請求項の数５　ＯＬ　（全 24 頁）

(21)出願番号　特願2001－252399(P2001－252399)

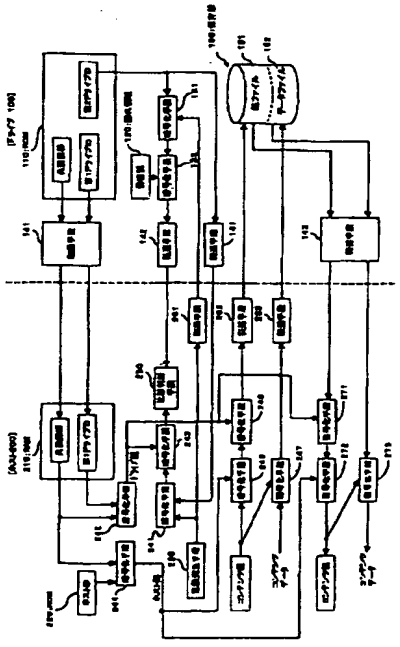
(22)出願日　平成13年８月23日(2001.8.23)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(72)発明者　岡田　佳之
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(74)代理人　100092978
弁理士　真田　有

最終頁に続く

(54)【発明の名称】　データ保護方法

(57)【要約】
【課題】ドライブ側での処理の負荷が大きくすることなく、ドライブのデータを不正なアクセスから保護し、ドライブ側での不正コピーのみならずホスト側での不正行為も確実に防止し、著作権を確実に保護できるようにするとともに、ドライブの不正転用も確実に防止できるようにする。
【解決手段】ホスト２００においてドライブ１００の認証を行ない、ドライブ１００が認証された場合、ホスト２００の記憶領域２２０に予め登録されているホストＩＤとドライブ１００の記憶領域１１０から読み出された共通鍵および第１識別情報とによりコンテンツ鍵を暗号化し、暗号化されたコンテンツ鍵をドライブ１００へ転送するとともに、ホスト２００においてドライブ１００に記録・保存すべきコンテンツデータをコンテンツ鍵により暗号化し、暗号化されたコンテンツデータをドライバ１００へ転送する。



【特許請求の範囲】
【請求項１】　データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該アクセス装置において該データ記録装置の認証を行なうステップと、
該データ記録装置が認証された場合、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報とにより、コンテンツ鍵を暗号化するステップと、
暗号化されたコンテンツ鍵を、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップと、
該アクセス装置において、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化するステップと、
暗号化されたコンテンツデータを、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴とする、データ保護方法。
【請求項２】　データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置に、コンテンツ鍵により暗号化されたコンテンツデータを書き込むとともに、所定のアクセス装置識別情報と該データ記録装置の記憶領域に予め登録されている共通鍵および第１識別情報とにより暗号化された該コンテンツ鍵を書き込むステップと、
該アクセス装置において該データ記録装置の認証を行なうステップと、
該データ記録装置が認証された場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、
該アクセス装置において、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報とにより、前記暗号化されたコンテンツ鍵を復号化するステップと、
復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとを含むことを特徴とする、データ保護方法。
【請求項３】　データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置が初期状態である時に該データ記録装置に最初に接続された該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報を、該アクセス装置から該データ記録装置へ転送し、１回のみ書込可能な記憶領域に書き込むステップと、
以後、該アクセス装置が該データ記録装置にアクセスする都度、該データ記録装置において、前記１回のみ書込可能な記憶領域に書き込まれた該アクセス装置識別情報に基づき、該アクセス装置の認証を行なうステップと、
該アクセス装置が認証された場合、該アクセス装置において該データ記録装置の認証を行なうステップと、
該データ記録装置が認証された場合で且つコンテンツデータを該データ記録装置に記録・保存する場合、該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報によりコンテンツ鍵を暗号化するステップと、
暗号化されたコンテンツ鍵を、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップと、
該アクセス装置において、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化するステップと、
暗号化されたコンテンツデータを、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴とする、データ保護方法。
【請求項４】　該アクセス装置および該データ記録装置がいずれも認証された場合で且つ該データ記録装置からコンテンツデータを読み出す場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、
該アクセス装置において、該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報により、前記暗号化されたコンテンツ鍵を復号化するステップと、
復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとをさらに含むことを特徴とする、請求項３記載のデータ保護方法。
【請求項５】　該アクセス装置の認証を行なうステップが、
該データ記録装置で乱数を発生するステップと、
該乱数を該データ記録装置から該アクセス装置へ転送するステップと、
該データ記録装置において、該アクセス装置識別情報を前記乱数により暗号化するステップと、
該アクセス装置において、該アクセス装置識別情報を該データ記録装置からの前記乱数により暗号化するステップと、
暗号化された該アクセス装置識別情報を該アクセス装置から該データ記録装置へ転送するステップと、
該アクセス装置からの前記暗号化されたアクセス装置識

別情報と該データ記録装置で暗号化されたアクセス装置識別情報とを比較し、一致するか否かを判断するステップとを含み、
これらのアクセス装置識別情報が一致すると判断された場合、該アクセス装置が認証されることを特徴とする、請求項３または請求項４に記載のデータ保護方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、データを記録・保存するデータ記録装置と、このデータ記録装置にアクセスするアクセス装置との間で音楽や映像などのデータを転送する際に、不正なアクセスからデータを保護するための方法に関する。ここで、データ記録装置は、例えば、音楽や映像などのデータを記録するデジタル録画再生装置であり、アクセス装置は、例えば、パーソナルコンピュータや、データ記録装置内のホスト（ＣＰＵ）である。
【０００２】近年、パソコンの性能向上やＭＰＥＧ２－ＩＳＩの出現で映像，音楽のデータを取り扱うことが容易になってきている。また、数１０ＧＢ（ギガバイト）の大容量ディスクが安価に手に入るようになり、ハードディスクドライブ（ＨＤＤ）あるいは光ディスクドライブをベースにした、新しいデジタル録画再生装置も登場してきている。
【０００３】このように安価で高性能のデータ記録装置を一般に広く普及させる際の鍵となるのが、そのデータ記録装置によって記録される各種データ（コンテンツ）の著作権の保護であり、不正コピーなどを確実に防止してコンテンツ提供者の権利を守る必要がある。本発明では、ホスト（アクセス装置）とドライブ（データ記録装置）との間でデータを転送する際、特に、ドライブ側に処理負担をかけることなく、データを不正なアクセスから保護し、著作権を確実に保護できるようにした技術を提供する。
【０００４】
【従来の技術】現状のデジタル録画再生装置としては、ＨＤＤレコーダや蓄積型セットトップボックス（ＳＴＢ）などがあるが、著作権保護の関係から、その装置に内蔵されたＨＤＤを、装置外へ取り出せないように機構的に固定化する立場が採られる場合が多い。一方、ユーザの立場からすれば、装置（ＨＤＤ以外の部分）はそのままにしながら、ＨＤＤの部分だけを、近年、容量が急激に増大しているＰＣ（Personal Computer）系の新型ＨＤＤに置き換えたいという要望が強い。
【０００５】その際、ホストとディスクドライブとの間のデータ転送時における著作権保護（つまり、不正なアクセスからのデータ保護）が課題となる。従来、ＰＣ系の標準インタフェース（ＡＴＡ／ＡＴＡＰＩ：Advanced Technologies Attachment／ＡＴＡ Packet Interface）を利用した著作権保護方法（データ保護方法）としては、ＣＰＰＭ（Content Protection for Prerecorded Media）やＣＰＲＭ（Content Protection for Recordable Media）が知られている。
【０００６】ＣＰＲＭでは、ドライブ内にドライブ固有のＩＤ（識別情報；媒体で言えばメディアＩＤ）が設定されており、ホストからディスクに対するコンテンツデータの書込は、以下のような手順〔ステップ(a1)～(a8)〕で行なわれる。
(a1)ホストからドライブに対して、ドライブ内のＲＯＭ領域に保存されている共通鍵群（複数のメディアキーブロック，複数の秘密鍵）および第１ドライブＩＤ（静的なＩＤ）の転送を要求する。
【０００７】(a2)ステップ(a1)の要求に応じて、共通鍵群および第１ドライブＩＤをドライブからホストへ転送する。
(a3)ホストのＲＡＭ領域に、ドライブからの共通鍵群および第１ドライブＩＤを格納する。
(a4)ホスト側で生成した乱数をドライブへ送るとともに、ホストからドライブに対して、生の第２ドライブＩＤ（動的なＩＤ）と、暗号化された第２ドライブＩＤとの転送を要求する。
【０００８】(a5)ステップ(a4)の要求に応じて、第２ドライブＩＤを、ホストからの乱数と、隠れ領域に既に書き込まれているドライブ鍵（秘密鍵）とにより暗号化し、生の第２ドライブＩＤと暗号化された第２ドライブＩＤとをドライブからホストへ転送する。
【０００９】(a6)ホストにおいて、ステップ(a3)で保存した共通鍵群および第１ドライブＩＤからドライブ鍵（相当）を作成し、そのドライブ鍵とステップ(a4)で生成した乱数とにより、ドライブからの生の第２ドライブＩＤを暗号化してから、ホスト側で暗号化された第２ドライブＩＤと、ドライブからの暗号化された第２ドライブＩＤとを比較し、これらが一致するか否かを判断する。
【００１０】(a7)ステップ(a6)で一致したと判断された場合には、ドライブ認証に成功したものと判断し、ドライブに書き込むべきコンテンツデータをコンテンツ鍵により暗号化するとともに、共通鍵群および第１ドライブＩＤから作成されたドライブ鍵（相当）によりコンテンツ鍵を暗号化する。そして、暗号化されたコンテンツデータおよび暗号化されたコンテンツ鍵を、ホストからドライブへ転送しディスクに書き込む。
(a8)ステップ(a6)で一致しないと判断された場合には、ドライブ認証に失敗したものと判断し、コンテンツデータをドライブに転送することなく処理を中断する。
【００１１】一方、ＣＰＲＭでは、上述のごとくディスクに書き込まれたコンテンツデータをディスクからホストへ読み出す際、上述と同様の手順〔ステップ(a1)～(a6)〕でドライブの認証を行なった後、以下のような手順〔ステップ(b1)および(b2)〕でコンテンツデータが読み

出される。
(b1)ステップ(a6)で一致したと判断された場合には、ドライブ認証に成功したものと判断し、ホストは、ドライブ（ディスク）から、暗号化されたコンテンツ鍵および暗号化されたコンテンツデータを読み出す。そして、共通鍵群および第１ドライブＩＤから作成されたドライブ鍵（相当）により、暗号化されたコンテンツ鍵を復号化してから、さらに、復号化されたコンテンツ鍵により、暗号化されたコンテンツデータを復号化する。
【００１２】(b2)ステップ(a6)で一致しないと判断された場合には、ドライブ認証に失敗したものと判断し、コンテンツをディスクから読み出すことなく処理を中断する。なお、ＣＰＰＭは、読出し専用の著作件保護方式であり、このＣＰＰＭでは、上述したステップ(a1)～(a6)，(b1)および(b2)が実行される。
【００１３】上述したドライブ認証手順〔ステップ(a1)～(a6)〕は、チャレンジ＆レスポンス方式と呼ばれ、ＣＰＲＭやＣＰＰＭでは、ホスト側のみで認証が行なわれている。つまり、単方向のドライブ認証が行なわれ、これにより、ドライブ側での処理の負担を軽減している。また、コンテンツ鍵やコンテンツデータがドライブ固有のＩＤに基づいてディスクに記録されているので、そのドライブのディスクに記録されたデータが別の媒体に不正にコピー（ボリュームコピー）されたとしても、データ読出に際してＩＤが一致しないため、不正コピーされたデータを読み出すことはできない。従って、ＣＰＲＭやＣＰＰＭは不正コピーの防止に有効である。
【００１４】ＣＰＲＭやＣＰＰＭ以外の著作権保護手法の代表的なものとしては、ＩＥＥＥ１３９４－ＩＦを利用したＤＴＣＰ（Digital Transmission Content Protection）がある。このＤＴＣＰは、装置間のデータ転送を想定しており、相互認証を基本としている。このＤＴＣＰとしては、フル認証（Full Authentication）方式と制限認証（Restrict Authentication）方式との２種類がある。フル認証方式では、公開鍵／秘密鍵暗号技術の電子署名アルゴリズムとＤＨ鍵交換アルゴリズムとが採用されており、いずれのアルゴリズムも楕円曲線暗号を基礎としている。
【００１５】ここで、ホストとディスクドライブとの間のデータ転送に際しフル認証方式のＤＴＣＰを用いた場合の、相互認証手順〔ステップ(c1)～(c9)〕について説明する。
(c1)ホストからドライブに対し、ホストの認証を要求する。このとき、ホストは、ドライブに乱数とホスト固有ＩＤとを送る。このホスト固有ＩＤは、ＤＴＣＰのライセンス組織（米国ＤＴＬＡ社）が機器毎に生成した証明情報であり、公開鍵や電子署名なども含まれる。
【００１６】(c2)ドライブは、ホストから乱数とホスト固有ＩＤとを受け取ると、ホスト固有ＩＤがＤＴＬＡ社作成の情報であるかを、電子署名の検証処理に従って確認するとともに、そのホスト固有ＩＤがドライブ側で保持される不正機器リストに載っていないかを調べる。
(c3)ステップ(c2)での確認の結果、何ら問題がなければ、ドライブからホストに対し、ドライブの認証を要求する。このとき、ドライブは、ホストに乱数とドライブ固有ＩＤを送る。このドライブ固有ＩＤも、ホスト固有ＩＤと同様、米国ＤＴＬＡ社が機器毎に生成した証明情報である。
【００１７】(c4)ホストは、ドライブから乱数とドライブ固有ＩＤとを受け取ると、ステップ(c2)と同様、ドライブ固有ＩＤがＤＴＬＡ社作成の情報であるかを、電子署名の検証処理に従って確認するとともに、そのドライブ固有ＩＤがホスト側で保持される不正機器リストに載っていないかを調べる。
(c5)ステップ(c4)での確認の結果、何ら問題がなければ、ＤＨ鍵交換方式（配送・共有方式）に従い、暗号鍵を共有するため、各装置（ホスト／ドライブ）において、その装置のＤＨ情報を計算する。
【００１８】(c6)ホストからドライブへ、ホストのＤＨ情報を送る。
(c7)ドライブは、ホストから受け取ったＤＨ情報が間違いなくホストから送られてきたデータであるかを、電子署名の検証に従って確認する。
(c8)逆に、ドライブからホストへ、ドライブのＤＨ情報を送る。
(c9)ホストは、ドライブから受け取ったＤＨ情報が間違いなくドライブから送られてきたデータであるかを、電子署名の検証に従って確認する。
【００１９】上述のように、ＤＴＣＰに代表される相互認証方式においては、ホストおよびドライブが、それぞれ、ドライブおよびホストがデータ転送を行なうのに正しい相手であるかどうかをチェックする機構（相互認証機構）を有しているので、ドライブ側での不正コピーが確実に防止されるだけでなく、ホスト側での不正行為（成りすまし等）も確実に防止することができる。
【００２０】なお、制限認証方式のＤＴＣＰは、共通の秘密鍵とハッシュ関数とを用いて認証を行なうものであるが、この制限認証方式のＤＴＣＰにおいても、基本的には上述したフル認証方式のＤＴＣＰと同様、ホストとドライブとは、対等な関係であり、相互に同様の認証処理を実行するので、その説明は省略する。
【００２１】
【発明が解決しようとする課題】しかしながら、上述したＣＰＲＭやＣＰＰＭでは、ホスト側でドライブの認証を行なうだけなので、ドライブ側での不正コピーを確実に防止することはできるが、ドライブ側でホストの認証を行なうことができない。従って、ドライブの認証が成立すれば、複数の装置（ホスト）から、つまり、正規ではないホストからも、そのドライブにアクセスし、ディスクに記録されたコンテンツデータを再生することが可

能になってしまう。このため、ドライブのデータを、正規ではないホストによる不正なアクセスから保護できず、ホスト側での不正行為（成りすまし等）を防止することができないという課題がある。

【００２２】そこで、上述したＤＴＣＰを採用することにより、ホスト側でドライブの認証が行なわれ且つドライブ側でホストの認証が行なわれるので、ドライブ側での不正コピーもホスト側での不正行為も防止することは可能になる。しかし、上述のごとくＤＴＣＰの認証処理は極めて複雑であり、ホストとドライブとが対等な関係であるため、特に、ドライブ側で複雑な認証処理を行なわなければならず、ドライブ側での処理の負荷が大きくなり好ましくない。

【００２３】また、近年、セットトップボックス（ＳＴＢ）を安価に貸し出すというビジネスが展開され始めているが、このようなビジネスの展開に伴い、ＳＴＢ内のハードディスクドライブに記録されたデータを不正コピーするだけでなく、そのハードディスクドライブそのものを抜き出してパソコンのドライブとして不正転用するという、不正利用者が出現してきている。

【００２４】このような不正利用者に対抗するために、上述したＤＴＣＰのような相互認証方式を採用することが望まれている。しかし、ＤＴＣＰでは、上述した通り、ＤＴＣＰの認証処理は極めて複雑で、ドライブ側での処理の負荷が大きくなる。このため、より簡易な処理で、且つ、ドライブ側での負荷を大きくすることなく、上述のような不正転用を確実に防止できるようにすることが望まれている。

【００２５】本発明は、このような課題に鑑み創案されたもので、ドライブ側での処理の負荷が大きくすることなく、データを不正なアクセスから保護し、データ記録装置（ドライブ）側での不正コピーのみならずアクセス装置（ホスト）側での不正行為をも確実に防止し、著作権を確実に保護できるようにするとともに、データ記録装置の不正転用も確実に防止できるようにした、データ保護方法を提供することを目的とする。

【００２６】

【課題を解決するための手段】上記目的を達成するために、本発明のデータ保護方法（請求項１）は、データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報とによりコンテンツ鍵を暗号化するステップと、暗号化されたコンテンツ鍵を該データ記録装置に書き込むべく該アクセス装置から該データ記録装置へ転送するステップと、該アクセス装置において該データ記録装置に記録・保存すべきコンテンツデータを該コンテンツ鍵により暗号化するステップと、暗号化されたコンテンツデータを該データ記録装置に書き込むべく該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴としている。

【００２７】また、本発明のデータ保護方法（請求項２）は、データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置に、コンテンツ鍵により暗号化されたコンテンツデータを書き込むとともに、所定のアクセス装置識別情報と該データ記録装置の記憶領域に予め登録されている共通鍵および第１識別情報とにより暗号化された該コンテンツ鍵を書き込むステップと、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、該アクセス装置において、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報とにより、前記暗号化されたコンテンツ鍵を復号化するステップと、復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとを含むことを特徴としている。

【００２８】さらに、本発明のデータ保護方法（請求項３）は、データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置が初期状態である時に該データ記録装置に最初に接続された該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報を、該アクセス装置から該データ記録装置へ転送し、１回のみ書込可能な記憶領域に書き込むステップと、以後、該アクセス装置が該データ記録装置にアクセスする都度、該データ記録装置において、前記１回のみ書込可能な記憶領域に書き込まれた該アクセス装置識別情報に基づき、該アクセス装置の認証を行なうステップと、該アクセス装置が認証された場合、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合で且つコンテンツデータを該データ記録装置に記録・保存する場合、該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報によりコンテンツ鍵を暗号化するステップと、暗号化されたコンテンツ鍵を、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップと、該アクセス装

置において、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化するステップと、暗号化されたコンテンツデータを、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴としている。

【００２９】このとき、該アクセス装置および該データ記録装置がいずれも認証された場合で且つ該データ記録装置からコンテンツデータを読み出す場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、該アクセス装置において、該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報により、前記暗号化されたコンテンツ鍵を復号化するステップと、復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとがさらに含まれていてもよい（請求項４）。

【００３０】また、該アクセス装置の認証を行なうステップが、該データ記録装置で乱数を発生するステップと、該乱数を該データ記録装置から該アクセス装置へ転送するステップと、該データ記録装置において、該アクセス装置識別情報を前記乱数により暗号化するステップと、該アクセス装置において、該アクセス装置識別情報を該データ記録装置からの前記乱数により暗号化するステップと、暗号化された該アクセス装置識別情報を該アクセス装置から該データ記録装置へ転送するステップと、該アクセス装置からの前記暗号化されたアクセス装置識別情報と該データ記録装置で暗号化されたアクセス装置識別情報とを比較し、一致するか否かを判断するステップとを含み、これらのアクセス装置識別情報が一致すると判断された場合に該アクセス装置を認証するように構成してもよい（請求項５）。

【００３１】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。

〔１〕第１実施形態の説明

図１は本発明の第１実施形態としてのデータ保護方法を適用されたデータ保護システム（アクセス装置およびデータ記録装置）の機能構成を示すブロック図であり、第１実施形態におけるデータ保護システムは、図１に示すように、データを記録・保存するデータ記録装置としてのドライブ（例えばＨＤＤ）１００と、このドライブ１００にアクセスするアクセス装置としてのホスト（例えばＣＰＵ）２００との間でデータ転送を行なう際に、ドライブ１００のデータを不正なアクセスから保護するためのものである。

【００３２】ドライブ１００は、ＲＯＭ１１０，隠れ領域１２０，暗号化手段１３１，１３２，転送手段１４１～１４３および保存部１５０をそなえて構成されている。ここで、ＲＯＭ（Read Only Memory；第１記憶領域）１１０は、共通鍵群，第１ドライブＩＤ（第１識別情報）および第２ドライブＩＤ（第２識別情報）を予め登録されて保持するものであり、隠れ領域１２０は、ドライブ鍵（秘密鍵）を予め登録されて保持するものである。

【００３３】暗号化手段１３１は、ＲＯＭ１１０から読み出された第２ドライブＩＤを、ホスト２００からの乱数により暗号化するものであり、暗号化手段１３２は、暗号化手段１３１による暗号化結果を、さらに、隠れ領域から読み出されたドライブ鍵（秘密鍵）により暗号化するものである。これらの暗号化手段１３１および１３２が、ホスト２００からの要求に応じて、第２ドライブＩＤを、当該要求とともにホスト２００から送られてくる乱数とドライブ１００のドライブ鍵（秘密鍵）とにより暗号化する第１暗号化手段として機能することになる。

【００３４】転送手段（第１転送手段）１４１は、ホスト２００からの要求に応じて、共通鍵群，第１ドライブＩＤおよび第２ドライブＩＤをＲＯＭ１１０から読み出してホスト２００へ転送するものである。転送手段（第２転送手段）１４２は、暗号化手段１３１および１３２により暗号化された第２ドライブＩＤをホスト２００へ転送するものである。転送手段（第３転送手段）１４３は、ホスト２００からの要求に応じて、暗号化コンテンツデータおよび暗号化コンテンツ鍵を保存部１５０から読み出してホスト２００へ転送するものである。

【００３５】保存部１５０は、ドライブ１００におけるディスク媒体そのものであり、ホスト２００からのコンテンツデータおよびコンテンツ鍵を書き込まれて保存するもので、コンテンツ鍵を保存する鍵ファイル１５１と、コンテンツデータを保存するデータファイル１５２とを有している。なお、保存部１５０に保存されるコンテンツデータは、コンテンツ鍵により暗号化されているとともに、保存部１５０に保存されるコンテンツ鍵は、後述するごとく、ホストＩＤ（所定のアクセス装置識別情報）とドライブ１００の共通鍵および第１ドライブＩＤとにより暗号化されている。

【００３６】一方、ホスト２００は、ＲＡＭ２１０，ＲＯＭ２２０，乱数発生手段２３０，暗号化手段２４１～２４７，比較判断手段２５０，転送手段２６１～２６３および復号化手段２７１～２７３をそなえて構成されている。ここで、ＲＡＭ（Random Access Memory）２１０は、ドライブ１００から転送されてきた共通鍵群および第１ドライブＩＤを一時的に保存するものであり、ＲＯＭ（Read Only Memory；第２記憶領域）２２０は、ホスト２００固有の識別情報であるホストＩＤ（アクセス装置識別情報）を予め登録されて保持するものである。

【００３７】乱数発生手段（第１乱数発生手段）２３０は、ホスト２００がドライブ１００に対してアクセスす

る際に乱数を発生するものである。暗号化手段２４１は、ドライブ１００から転送されてきた生の第２ドライブＩＤを、乱数発生手段２３０で生成された乱数により暗号化するものであり、暗号化手段２４２は、ＲＡＭ２１０に保存された第１ドライブＩＤを、ＲＡＭ２１０に保存された共通鍵群により暗号化することによって、ドライブ鍵（相当）を生成・出力するものであり、暗号化手段２４３は、暗号化手段２４１による暗号化結果を、さらに、暗号化手段２４２からのドライブ鍵（相当）により暗号化するものである。

【００３８】これらの暗号化手段２４１～２４３が、ドライブ１００のＲＯＭ１１０から読み出された第２ドライブＩＤを、乱数発生手段２３０で発生された乱数と、ドライブ１００のＲＯＭ１１０から読み出された共通鍵群および第１ドライブＩＤとにより暗号化する第２暗号化手段として機能することになる。比較判断手段（第１比較判断手段）２５０は、ドライブ１００から転送手段１４２を通じて転送されてくる、暗号化された第２ドライブＩＤと、暗号化手段２４１～２４３によって暗号化された第２ドライブＩＤとを比較し、一致するか否かを判断するものである。

【００３９】そして、ホスト２００がドライブ１００（保存部１５０）にコンテンツデータを記録・保存する際、比較判断手段２５０により２種類の第２ドライブＩＤが一致すると判断された場合に、後述する暗号化手段２４４～２４７および転送手段２６１～２６３が動作するようになっている。また、ホスト２００がドライブ１００（保存部１５０）からコンテンツデータを読み出す際、比較判断手段２５０により２種類の第２ドライブＩＤが一致すると判断された場合に、後述する復号化手段２７１～２７３が動作するようになっている。

【００４０】暗号化手段２４４は、ＲＯＭ２２０に保存されたホストＩＤを、ＲＡＭ２１０に保存された共通鍵群により暗号化することによって、ホスト鍵を生成・出力するものであり、暗号化手段２４５は、コンテンツ鍵を、暗号化手段２４４の暗号化結果であるホスト鍵により暗号化するものであり、暗号化手段２４６は、暗号化手段２４５の暗号化結果を、さらに、暗号化手段２４２からのドライブ鍵（相当）により暗号化するものである。

【００４１】２種類の第２ドライブＩＤが一致すると比較判断手段２５０が判断した場合、上述した暗号化手段２４４～２４６および暗号化手段２４２が、ＲＯＭ２２０から読み出されたホストＩＤと、ＲＡＭ２１０に保存されている共通鍵群および第１ドライブＩＤとにより、コンテンツ鍵を暗号化する第３暗号化手段として機能することになる。

【００４２】暗号化手段（第４暗号化手段）２４７は、ドライブ１００に記録・保存すべきコンテンツデータを、コンテンツ鍵により暗号化するものである。転送手段（第４転送手段）２６１は、乱数発生手段２３０で発生された乱数をドライブ１００（暗号化手段１３１）へ転送するものである。

【００４３】転送手段（第５転送手段）２６２は、暗号化手段２４２および２４４～２４６により暗号化されたコンテンツ鍵を、ドライブ１００の保存部１５０（鍵ファイル１５１）に書き込むべく、ドライブ１００へ転送するものである。転送手段（第６転送手段）２６３は、暗号化手段２４７により暗号化されたコンテンツデータを、ドライブ１００の保存部１５０（データファイル１５２）に書き込むべく、ドライブ１００へ転送するものである。

【００４４】復号化手段２７１は、ドライブ１００の保存部１５０（鍵ファイル１５１）から読み出された暗号化コンテンツ鍵を、暗号化手段２４２からのドライブ鍵（相当）により復号化するものであり、復号化手段２７２は、復号化手段２７１による復号化結果を、さらに、暗号化手段２４４からのホスト鍵により復号化するものである。

【００４５】２種類の第２ドライブＩＤが一致すると比較判断手段２５０が判断した場合、上述した復号化手段２７１および２７２が、ＲＯＭ２２０から読み出されたホストＩＤと、ＲＡＭ２１０に保存されている共通鍵群および第１ドライブＩＤとにより、ドライブ１００の保存部１５０（鍵ファイル１５１）から読み出された暗号化コンテンツ鍵を復号化する第１復号化手段として機能することになる。

【００４６】復号化手段（第２復号化手段）２７３は、復号化手段２７１および２７２により復号化されたコンテンツ鍵により、ドライブ１００の保存部１５０（データファイル１５２）から読み出された暗号化コンテンツデータを復号化するものである。

【００４７】上述したホスト２００における乱数発生手段２３０，暗号化手段２４１～２４７，比較判断手段２５０，転送手段２６１～２６３および復号化手段２７１～２７３としての機能は、専用ソフトウェア（アクセスプログラム）によって実現される。このアクセスプログラムは、例えばフレキシブルディスク，ＣＤ－ＲＯＭ等のコンピュータ読取可能な記録媒体に記録された形態で提供される。第１実施形態においては、ホスト２００を成すＲＯＭ（Read Only Memory）等に予めアクセスプログラムを格納しておき、このアクセスプログラムを、ホスト２００を成すＣＰＵによって読み出し実行することで、上述した乱数発生手段２３０，暗号化手段２４１～２４７，比較判断手段２５０，転送手段２６１～２６３および復号化手段２７１～２７３としての機能が実現される。なお、アクセスプログラムは、例えば磁気ディスク，光ディスク，光磁気ディスク等の記憶装置（記録媒体）に記録しておき、その記憶装置から通信経路を介してコンピュータに提供されてもよい。また、ドライブ１

００における暗号化手段１３１，１３２および転送手段１４１，１４２としての機能も、専用ソフトウェアによって実現される。

【００４８】なお、ドライブ１００においては、ドライブ１００からホスト２００へ転送するデータの種類毎に、転送手段１４１～１４３をそなえているが、実際には、これらの転送手段１４１～１４３としての機能を一つの転送手段によって実現してもよい。また、暗号化手段１３１および１３２としての機能も一つの暗号化手段によって実現してもよい。

【００４９】同様に、ホスト２００においては、ホスト２００からドライブ１００へ転送するデータの種類毎に、転送手段２６１～２６３をそなえているが、実際には、これらの転送手段２６１～２６３としての機能を一つの転送手段によって実現してもよい。また、暗号化手段２４１～２４７としての機能も一つの暗号化手段によって実現してもよいし、復号化手段２７１～２７３としての機能も一つの復号化手段によって実現してもよい。

【００５０】次に、上述のごとく構成された第１実施形態のデータ保護システムの動作について、図２～図５を参照しながら説明する。なお、図２は第１実施形態のデータ保護システムにおけるコンテンツデータ書込動作に係る要部を取り出して示すブロック図、図３は第１実施形態におけるコンテンツデータ書込手順を説明するための図、図４は第１実施形態のデータ保護システムにおけるコンテンツデータ読出動作に係る要部を取り出して示すブロック図、図５は第１実施形態におけるコンテンツデータ読出手順を説明するための図である。

【００５１】第１実施形態では、前述したＣＰＲＭの手法を用いながら、コンテンツデータおよびコンテンツ鍵を書き込む際に、コンテンツ鍵をホスト固有のＩＤを用いて暗号化している。つまり、第１実施形態では、ドライブ１００内にドライブ固有の第１ドライブＩＤおよび第２ドライブＩＤが設定されるとともに、ホスト２００内にホスト固有のホストＩＤが設定されており、ホスト２００からドライブ１００（保存部１５０）に対するコンテンツデータの書込は、以下のような手順〔ステップ(A1)～(A11)〕で行なわれる。なお、図２および図３においては、ステップ(A1)～(A11)に対応する処理を行なっている箇所に、それぞれ(A1)～(A11)が符号として記入されている。

【００５２】(A1)ホスト２００からドライブ１００に対して、ドライブ１００内のＲＯＭ１１０領域に保存されている共通鍵群（複数のメディアキーブロック，複数の秘密鍵）および第１ドライブＩＤ（静的なＩＤ）の転送を要求する。

(A2)ステップ(A1)の要求に応じて、共通鍵群および第１ドライブＩＤを、ＲＯＭ１１０から読み出し、ドライブ１００からホスト２００へ転送する（図１の転送手段１４１の機能）。

【００５３】(A3)ホスト２００のＲＡＭ２１０に、ドライブ１００からの共通鍵群および第１ドライブＩＤを格納・保持する。

(A4)ホスト２００側の乱数発生手段２３０で乱数を発生し、その乱数をドライブ１００へ送るとともに（図１の転送手段２６１の機能）、ホスト２００からドライブ１００に対して、生の第２ドライブＩＤ（動的なＩＤ）とその第２ドライブＩＤを上記乱数により暗号化したものとを転送するように要求する。

【００５４】(A5)ステップ(A4)の要求に応じて、暗号化手段１３１および１３２が、第２ドライブＩＤを、ホスト２００からの乱数と、隠れ領域１２０に書き込まれているドライブ鍵（秘密鍵）とにより暗号化する。そして、生の第２ドライブＩＤと暗号化された第２ドライブＩＤとをドライブ１００からホスト２００へ転送する（図１の転送手段１４１，１４２の機能）。

【００５５】(A6)ホスト２００において、暗号化手段２４２が、ステップ(A3)で保存した共通鍵群と第１ドライブＩＤとに基づきドライブ鍵（相当）を作成し、そのドライブ鍵とステップ(A4)で生成した乱数とにより、ドライブ１００からの生の第２ドライブＩＤを暗号化する。そして、比較判断手段２５０において、ホスト２００側で暗号化された第２ドライブＩＤと、ドライブ１００からの暗号化された第２ドライブＩＤとを比較し、これらが一致するか否かを判断する。第１実施形態では、上記ステップ(A1)～(A6)により、ドライブ１００の認証がホスト２００側で行なわれる。

【００５６】(A7)ステップ(A6)で一致したと判断された場合には、ドライブ１００の認証に成功したものと判断し、暗号化手段２４２および２４４～２４６が、ＲＯＭ２２０から読み出されたホストＩＤと、ＲＡＭ２１０に保存されている共通鍵群および第１ドライブＩＤとにより、コンテンツ鍵を暗号化する。つまり、ホストＩＤと共通鍵群とから生成されたホスト鍵と、第１ドライブＩＤと共通鍵群とから生成されたドライブ鍵（相当）とによって、コンテンツ鍵が暗号化される。

【００５７】(A8)ステップ(A7)で暗号化されたコンテンツ鍵を、ホスト２００からドライブ１００へ転送し（図１の転送手段２６２の機能）、ドライブ１００の保存部１５０（鍵ファイル１５１）に書き込む。

(A9)ステップ(A6)で一致したと判断された場合、上述したステップ(A7)，(A8)の処理と並行して、暗号化手段２４７が、ドライブ１００に書き込むべきコンテンツデータをコンテンツ鍵により暗号化する。

【００５８】(A10)ステップ(A9)で暗号化されたコンテンツデータを、ホスト２００からドライブ１００へ転送し（図１の転送手段２６３の機能）、ドライブ１００の保存部１５０（データファイル１５２）に書き込む。

(A11)ステップ(A6)で一致しないと判断された場合には、ドライブ認証に失敗したものと判断し、上述したス

テップ(A7)～(A10)の処理を行なうことなく、処理を中断する。

【００５９】一方、上述のごとくドライブ１００の保存部１５０に書き込まれたコンテンツデータをドライブ１００からホスト２００へ読み出す際、第１実施形態では、上述と同様のステップ(A1)～(A6)に従ってドライブ１００の認証を行なった後、以下のような手順〔ステップ(B1)～(B6)〕でコンテンツデータが読み出される。なお、図４および図５においては、ステップ(A1)～(A6)および(B1)～(B5)に対応する処理を行なっている箇所に、それぞれ(A1)～(A6)および(B1)～(B5)が符号として記入されている。ここで、ステップ(A1)～(A6)によるドライブ認証手順は上述と同様であるので、その説明は省略する。

【００６０】(B1)ステップ(A6)で一致したと判断された場合には、ドライブ認証に成功したものと判断し、ホスト２００は、ドライブ１００に対し、暗号化コンテンツ鍵および暗号化コンテンツデータの読出を要求する。

(B2)ステップ(B1)の要求に応じて、ドライブ１００は、暗号化コンテンツ鍵および暗号化コンテンツを保存部１５０から読み出してホスト２００へ転送する（図１の転送手段１４３の機能）。

【００６１】(B3)ホスト２００においては、復号化手段２７１および２７２が、ＲＯＭ２２０から読み出されたホストＩＤと、ＲＡＭ２１０に保存されている共通鍵群および第１ドライブＩＤとにより、ドライブ１００の保存部１５０（鍵ファイル１５１）から読み出された暗号化コンテンツ鍵を復号化する。つまり、ホストＩＤと共通鍵群とから生成されたホスト鍵と、第１ドライブＩＤと共通鍵群とから生成されたドライブ鍵（相当）とによって、暗号化されたコンテンツ鍵が復号化される。

【００６２】(B4)そして、復号化手段２７３が、復号化手段２７１および２７２で復号化されたコンテンツ鍵により、ドライブ１００の保存部１５０（データファイル１５２）から読み出された暗号化コンテンツデータを復号化する。

(B5)ステップ(A6)で一致しないと判断された場合には、ドライブ認証に失敗したものと判断し、上述したステップ(B1)～(B4)の処理を行なうことなく、処理を中断する。

【００６３】(B6)コンテンツ鍵を暗号化してドライブ１００に書き込んだホスト２００とは異なるホストが、コンテンツ鍵を復号化しようとした場合、復号化に用いられるホストＩＤが、暗号化に用いられたホストＩＤとは異なってしまう。このような場合、ステップ(B3)において正しいコンテンツ鍵が復元されないので、ステップ(B4)において暗号化コンテンツデータを復号化することができず、ホスト２００は、本来のコンテンツデータを得ることができなくなる。

【００６４】このように、本発明の第１実施形態としてのデータ保護システムによれば、ホスト２００がコンテンツデータおよびコンテンツ鍵をドライブ１００に書き込む際に、コンテンツ鍵が、ドライブ１００の識別情報（第１ドライブＩＤ）にホストＩＤの要素を加えて暗号化されているので、コンテンツデータやコンテンツ鍵をドライブ１００に書き込んだ正規のホスト２００しか、そのコンテンツデータを読み出すことができない。

【００６５】つまり、正規のホスト２００以外のホスト（ＣＰＵ等）がドライブ１００からコンテンツデータを読み出しても、そのホストの識別情報（ホストＩＤ）が正規のものと異なっているため、コンテンツ鍵を正しく復号化することができないので、コンテンツデータを正しく復号化できず、コンテンツデータを読み出すことができなくなる。

【００６６】従って、ＣＰＰＭやＣＰＲＭ等の単方向認証を採用してドライブ１００側での処理の負荷を大きくすることなく、ホスト２００とドライブ１００とを１対１で対応させる専用接続の形態が実現され、ドライブ１００のデータを不正なアクセスから保護することができるので、ドライブ１００側での不正コピーのみならず、ホスト２００側での成りすまし等によるデータの不正読出しや不正コピーをも確実に防止し、著作権を確実に保護することができる。

【００６７】〔２〕第２実施形態の説明

図６は本発明の第２実施形態としてのデータ保護方法を適用されたデータ保護システム（アクセス装置およびデータ記録装置）の機能構成を示すブロック図であり、第２実施形態におけるデータ保護システムも、第１実施形態とほぼ同様に構成されているが、図６に示すように、第２実施形態におけるデータ保護システムのドライブ（データ記録装置）１００Ａは、第１実施形態のドライブ１００に、暗号化手段１３３，転送手段１４４，１回書込可能記憶領域１６０，乱数発生手段１７０および比較判断手段１８０をさらにそなえて構成されている。また、第２実施形態におけるデータ保護システムのホスト（アクセス装置）２００Ａは、第１実施形態のホスト２００に、暗号化手段２４８，転送手段２６４および転送手段２６５をさらにそなえて構成されている。なお、図中、既述の符号と同一の符号は、同一もしくはほぼ同一の部分を示しているので、その説明は省略する。

【００６８】ここで、ドライブ１００Ａにおいて、１回書込可能記憶領域１６０は、ドライブ１００Ａが初期状態の時にこのドライブ１００Ａに最初に接続されたホスト２００Ａのホストｉｄを書き込まれるもので、データを１回だけ書き込むことができる領域である。乱数発生手段（第２乱数発生手段）１７０は、ホスト２００Ａからアクセスされる都度、乱数を発生するものである。

【００６９】転送手段（第７転送手段）１４４は、乱数発生手段１７０で発生された乱数をホスト２００Ａへ転送するものである。暗号化手段（第５暗号化手段）１３

３は、１回書込可能記憶領域１６０から読み出されたホストＩＤを、乱数発生手段１７０で発生された乱数により暗号化するものである。

【００７０】比較判断手段（第２比較判断手段）１８０は、暗号化手段１３３で暗号化されたホストＩＤと、後述するごとくホスト２００Ａから転送されてきた暗号化ホストＩＤとを比較し、一致するか否かを判断するものである。一方、ホスト２００Ａにおいて、暗号化手段（第６暗号化手段）２４８は、ＲＯＭ２２０に保存されているホストＩＤを、ドライブ１００Ａから転送手段１４４を通じて送られてくる乱数により暗号化するものである。

【００７１】転送手段（第８転送手段）２６４は、初期状態のドライブ１００Ａに最初に接続された時に、ホストＩＤをドライブ１００Ａの１回書込可能記憶領域１６０に書き込むべく、ホストＩＤをＲＯＭ２２０から読み出してドライブ１００Ａへ転送するものである。転送手段（第９転送手段）２６５は、ホスト２００Ａがドライブ１００Ａにアクセスする都度、暗号化手段２４８により暗号化されたホストＩＤをドライブ１００Ａ（比較判断手段１８０）へ転送するものである。

【００７２】そして、第２実施形態のデータ保護システムにおいては、ホスト２００Ａがドライブ１００Ａ（保存部１５０）にコンテンツデータを記録・保存する際、比較判断手段２５０および１８０がいずれも識別情報が一致すると判断した場合に、暗号化手段２４２，２４４～２４７，転送手段２６２および２６３が動作するようになっている。また、ホストＡ２００がドライブ１００Ａ（保存部１５０）からコンテンツデータを読み出す際、比較判断手段２５０により２種類の第２ドライブＩＤが一致すると判断された場合に、後述する復号化手段２７１～２７３が動作するようになっている。

【００７３】上述のごとく第２実施形態のドライブ１００Ａにおいて新たに追加された、暗号化手段１３３，転送手段１４４，乱数発生手段１７０および比較判断手段１８０としての機能も、専用ソフトウェアによって実現される。同様に、第２実施形態のホスト２００Ａにおいて新たに追加された、暗号化手段２４８，転送手段２６４および転送手段２６５としての機能も、専用ソフトウェア（アクセスプログラム）によって実現される。

【００７４】なお、ドライブ１００Ａにおいては、転送手段１４４としての機能を、第１実施形態で説明した転送手段１４１～１４３としての機能とともに、一つの転送手段によって実現してもよい。また、暗号化手段１３３としての機能を、第１実施形態で説明した暗号化手段１３１および１３２としての機能とともに、一つの暗号化手段によって実現してもよい。

【００７５】同様に、ホスト２００Ａにおいては、転送手段２６４および２６５としての機能を、第１実施形態で説明した転送手段２６１～２６３としての機能とともに、一つの転送手段によって実現してもよい。また、暗号化手段２４８としての機能を、第１実施形態で説明した暗号化手段２４１～２４７としての機能とともに、一つの暗号化手段によって実現してもよい。

【００７６】次に、上述のごとく構成された第２実施形態のデータ保護システムの動作について、図７～図１０を参照しながら説明する。なお、図７は第２実施形態のデータ保護システムにおけるコンテンツデータ書込動作に係る要部を取り出して示すブロック図、図８は第２実施形態におけるコンテンツデータ書込手順を説明するための図、図９は第２実施形態のデータ保護システムにおけるコンテンツデータ読出動作に係る要部を取り出して示すブロック図、図１０は第２実施形態におけるコンテンツデータ読出手順を説明するための図である。

【００７７】第２実施形態では、前述した第１実施形態と同様の手順でホスト２００Ａはドライブ１００Ａに対してアクセスしているが、そのアクセスに先立ち、ドライブ１００Ａ側でホスト２００Ａの認証を以下のような手順〔ステップ(C1)～(C7)〕で行なっている。ホスト認証後に、ホスト２００Ａからドライブ１００Ａ（保存部１５０）に対するコンテンツデータの書込は、第１実施形態と同様の手順〔ステップ(C8)～(C18)〕で行なわれる。なお、図７および図８においては、ステップ(C1)～(C18)に対応する処理を行なっている箇所に、それぞれ(C1)～(C18)が符号として記入されている。

【００７８】(C1)ホスト２００Ａがドライブ１００Ａにアクセスした際、そのドライブ１００Ａ（１回書込可能記憶領域１６０）が何も書き込まれていない初期状態であるか否かを認識し、初期状態である場合、ホストＩＤを、ＲＯＭ２２０から読み出し、ホスト２００Ａからドライブ１００Ａへ転送する（図６の転送手段２６４の機能）。

【００７９】(C2)ステップ(C1)でホスト２００Ａからドライブ１００Ａへ送られてきたホストＩＤを１回書込可能記憶領域１６０に書き込み保持する。このとき、記憶領域１６０に書き込まれたホストＩＤを、以降、ホストＩＤ－１と標記する。

(C3)上述したステップ(C1)および(C2)を実行した後、もしくは、ステップ(C1)でドライブ１Ａが初期状態ではないと認識された場合、ホスト２００Ａは、ドライブ１００Ａに対してホスト認証を依頼する。

【００８０】(C4)ホスト２００Ａからホスト認証の依頼を受けたドライブ１００Ａにおいては、乱数発生手段１７０で乱数を発生し、その乱数をホスト２００Ａへ送るとともに（図６の転送手段１４４の機能）、ドライブ１００Ａからホスト２００Ａに対し、ホストＩＤを上記乱数により暗号化したものを転送するように要求する。また、暗号化手段１３３が、乱数発生手段１７０で生成された乱数により、記憶領域１６０に書き込まれているホストＩＤ－１を暗号化する。

【００８１】(C5)ステップ(C4)の要求に応じて、暗号化手段２４８が、ＲＯＭ２２０に保持されているホストＩＤ（このホストＩＤを、以降、ホストＩＤ－２と標記する）を、ドライブ１００Ａからの乱数により暗号化する。そして、暗号化されたホストＩＤ－２をホスト２００Ａからドライブ１００Ａへ転送する（図６の転送手段２６５の機能）。

【００８２】(C6)そして、ドライブ１００Ａの比較判断手段１８０において、ステップ(C4)で得られた暗号化ホストＩＤ－１と、ホスト２００Ａからの暗号化されたホストＩＤ－２とを比較し、これらが一致するか否かを判断する。第２実施形態では、ステップ(C1)および(C2)により初期状態のドライブ１００Ａの記憶領域１６０にホストＩＤ－１が書き込まれた後は、ホスト２００Ａやそれ以外のホストがドライブ１００Ａにアクセスする都度、ドライブ１００Ａにおいて、記憶領域１６０に書き込まれたホストＩＤ－１に基づき、ホスト認証が行なわれる。

【００８３】(C7)ステップ(C6)で一致しないと判断された場合には、ホスト認証に失敗したものと判断し、処理を中断する。ステップ(C6)で一致したと判断された場合には、ホスト２００Ａの認証に成功したものと判断し、第１実施形態と同様にして、ホスト２００Ａからドライブ１００Ａ（保存部１５０）に対するコンテンツデータの書込が行なわれる。なお、以下のステップ(C8)～(C18)はそれぞれ第１実施形態のステップ(A1)～(A11)に対応している。

【００８４】(C8)ホスト２００Ａからドライブ１００Ａに対して、ドライブ１００Ａ内のＲＯＭ１１０領域に保存されている共通鍵群（複数のメディアキーブロック，複数の秘密鍵）および第１ドライブＩＤ（静的なＩＤ）の転送を要求する。(C9)ステップ(A1)の要求に応じて、共通鍵群および第１ドライブＩＤを、ＲＯＭ１１０から読み出し、ドライブ１００Ａからホスト２００Ａへ転送する（図６の転送手段１４１の機能）。

【００８５】(C10)ホスト２００ＡのＲＡＭ２１０に、ドライブ１００Ａからの共通鍵群および第１ドライブＩＤを格納・保持する。

(C11)ホスト２００Ａ側の乱数発生手段２３０で乱数を発生し、その乱数をドライブ１００Ａへ送るとともに（図６の転送手段２６１の機能）、ホスト２００Ａからドライブ１００Ａに対して、生の第２ドライブＩＤ（動的なＩＤ）とその第２ドライブＩＤを上記乱数により暗号化したものとの転送を要求する。

【００８６】(C12)ステップ(C11)の要求に応じて、暗号化手段１３１および１３２が、第２ドライブＩＤを、ホスト２００Ａからの乱数と、隠れ領域１２０に書き込まれているドライブ鍵（秘密鍵）とにより暗号化する。そして、生の第２ドライブＩＤと暗号化された第２ドライブＩＤとをドライブ１００Ａからホスト２００Ａへ転送する（図６の転送手段１４１，１４２の機能）。

【００８７】(C13)ホスト２００Ａにおいて、暗号化手段２４２が、ステップ(C10)で保存した共通鍵群と第１ドライブＩＤとに基づきドライブ鍵（相当）を作成し、そのドライブ鍵とステップ(C11)で生成した乱数とにより、ドライブ１００Ａからの生の第２ドライブＩＤを暗号化する。そして、比較判断手段２５０において、ホスト２００Ａ側で暗号化された第２ドライブＩＤと、ドライブ１００Ａからの暗号化された第２ドライブＩＤとを比較し、これらが一致するか否かを判断する。第１実施形態では、上記ステップ(C8)～(C13)により、ドライブ１００Ａの認証が行なわれる。

【００８８】(C14)ステップ(C13)で一致したと判断された場合には、ドライブ１００Ａの認証に成功したものと判断し、暗号化手段２４２および２４４～２４６が、ＲＯＭ２２０から読み出されたホストＩＤと、ＲＡＭ２１０に保存されている共通鍵群および第１ドライブＩＤとにより、コンテンツ鍵を暗号化する。つまり、ホストＩＤと共通鍵群とから生成されたホスト鍵と、第１ドライブＩＤと共通鍵群とから生成されたドライブ鍵（相当）とによって、コンテンツ鍵が暗号化される。

【００８９】(C15)ステップ(C14)で暗号化されたコンテンツ鍵を、ホスト２００Ａからドライブ１００Ａへ転送し（図１の転送手段２６２の機能）、ドライブ１００Ａの保存部１５０（鍵ファイル１５１）に書き込む。

(C16)ステップ(C13)で一致したと判断された場合、上述したステップ(C14)，(C15)の処理と並行して、暗号化手段２４７が、ドライブ１００に書き込むべきコンテンツデータをコンテンツ鍵により暗号化する。

【００９０】(C17)ステップ(C16)で暗号化されたコンテンツデータを、ホスト２００Ａからドライブ１００Ａへ転送し（図１の転送手段２６３の機能）、ドライブ１００Ａの保存部１５０（データファイル１５２）に書き込む。

(C18)ステップ(C13)で一致しないと判断された場合には、ドライブ認証に失敗したものと判断し、上述したステップ(C14)～(C17)の処理を行なうことなく、処理を中断する。

【００９１】一方、上述のごとくドライブ１００Ａの保存部１５０に書き込まれたコンテンツデータをドライブ１００Ａからホスト２００Ａへ読み出す際、第２実施形態では、上述と同様のステップ(C1)～(C7)に従ってホスト２００Ａの認証をドライブ１００Ａ側で行ない、さらに、上述と同様のステップ(C8)～(C13)に従ってドライブ１００Ａの認証をホスト２００Ａ側で行なった後、以下のような手順〔ステップ(D1)～(D5)〕でコンテンツデータが読み出される。

【００９２】なお、図９および図１０においては、ステップ(C1)～(C13)および(D1)～(D4)に対応する処理を行なっている箇所に、それぞれ(C1)～(C13)および(D1)～

(D4)が符号として記入されている。ここで、ステップ(C1)～(C7)によるホスト認証手順およびステップ(C8)～(C13)によるドライブ認証手順は、上述と同様であるので、その説明は省略する。なお、以下のステップ(D1)～(D5)はそれぞれ第１実施形態のステップ(B1)～(B5)に対応している。

【００９３】(D1)ステップ(C13)で一致したと判断された場合には、ドライブ認証に成功したものと判断し、ホスト２００Ａは、ドライブ１００Ａに対し、暗号化コンテンツ鍵および暗号化コンテンツデータの読出を要求する。

(D2)ステップ(D1)の要求に応じて、ドライブ１００Ａは、暗号化コンテンツ鍵および暗号化コンテンツを保存部１５０から読み出してホスト２００Ａへ転送する（図６の転送手段１４３の機能）。

【００９４】(D3)ホスト２００Ａにおいては、復号化手段２７１および２７２が、ＲＯＭ２２０から読み出されたホストＩＤと、ＲＡＭ２１０に保存されている共通鍵群および第１ドライブＩＤとにより、ドライブ１００Ａの保存部１５０（鍵ファイル１５１）から読み出された暗号化コンテンツ鍵を復号化する。つまり、ホストＩＤと共通鍵群とから生成されたホスト鍵と、第１ドライブＩＤと共通鍵群とから生成されたドライブ鍵（相当）とによって、暗号化されたコンテンツ鍵が復号化される。

【００９５】(D4)そして、復号化手段２７３が、復号化手段２７１および２７２で復号化されたコンテンツ鍵により、ドライブ１００Ａの保存部１５０（データファイル１５２）から読み出された暗号化コンテンツデータを復号化する。

(D5)ステップ(C13)で一致しないと判断された場合には、ドライブ認証に失敗したものと判断し、上述したステップ(D1)～(D4)の処理を行なうことなく、処理を中断する。

【００９６】このように、本発明の第２実施形態としてのデータ保護システムによれば、ドライブ１００Ａが初期状態である時にこのドライブ１００Ａに最初に接続されたホスト２００Ａの識別情報（ホストＩＤ－１）が、ドライブ１００Ａにおける１回書込可能記憶領域１６０に書き込まれ、それ以降、その記憶領域１６０に書き込まれたホストＩＤ－１に基づいて、ドライブ１００Ａにアクセスしたホスト２００Ａが、当該ドライブ１００Ａに最初に接続されたホスト２００Ａ（正規のホスト）であるかどうかの認証が行なわれる。そして、正規のホスト２００Ａであると認証された場合のみ、ドライブ１００Ａに対するアクセス（データ書込／読出）が許可される。

【００９７】これにより、ドライブ１００Ａ側で極めて簡素な認証処理を行なうだけで、正規のホスト２００Ａ以外のホストはドライブ１００Ａにアクセスすることができなくなる。従って、ドライブ１００Ａ側での処理の負荷を大きくすることなく、ドライブ１００Ａのデータを不正なアクセスから保護することができ、ドライブ１００Ａ側での不正コピーのみならず、ホスト２００Ａ側での成りすまし等によるデータの不正読出しや不正コピーをも確実に防止し、著作権を確実に保護することができる。

【００９８】さらに、ドライブ１００Ａに最初に接続された正規のホスト２００Ａしかドライブ１００Ａにアクセスすることができなくなるので、例えばＳＴＢからハードディスクドライブ（データ記録装置）を取り外しＳＴＢ以外のシステムで転用するといった、ドライブ１００Ａの不正転用をも確実に防止することができる。

【００９９】なお、第２実施形態のデータ保護システムにおいては、第１実施形態で説明した技術（つまりドライブ１００Ａに書き込むべきコンテンツ鍵を第１ドライブＩＤおよびホストＩＤにより暗号化する技術）も組み込まれている。これにより、例え何らかの手段を用いてホスト認証を不正にくぐり抜けたとしても、正規のホスト２００Ａ以外のホストでは、ドライブ１００Ａから読み出されたコンテンツ鍵を復号化することができず、コンテンツデータを読み出せない。従って、ホスト２００Ａ側での成りすまし等によるデータの不正読出しや不正コピーをより確実に防止することができる。

【０１００】〔３〕その他

本発明は上述した実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲で種々変形して実施することができる。例えば、上述した第２実施形態のデータ保護システムでは、アクセス毎にドライバ１００Ａ側でホスト認証を行なう技術と第１実施形態で説明した技術とを組み合わせているが、アクセス毎にドライバ１００Ａ側でホスト認証を行なう技術を、通常のＣＰＲＭやＣＰＰＭと組み合わせてもよい。具体的には、ステップ(C1)～(C7)を実行した後、第２実施形態におけるステップ(C8)～(C18)，(D1)～(D5)に代えて、ステップ(a1)～(a8)，(b1)，(b2)を実行してもよい。この場合でも、第２実施形態と同様の作用効果を十分に得ることができる。

【０１０１】また、第１実施形態や第２実施形態におけるドライブ認証手法は、上述したステップ(A1)～(A6)やステップ(C8)～(C13)による手法に限定されるものではない。同様に、第２実施形態におけるホスト認証手法も、上述したステップ(C1)～(C7)による手法に限定されるものではない。

【０１０２】〔４〕付記

（付記１）　データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合、該アクセス装置の記憶領域に予め登録されているアクセス

装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報とにより、コンテンツ鍵を暗号化するステップと、暗号化されたコンテンツ鍵を、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップと、該アクセス装置において、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化するステップと、暗号化されたコンテンツデータを、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴とする、データ保護方法。

【０１０３】（付記２）　データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置に、コンテンツ鍵により暗号化されたコンテンツデータを書き込むとともに、所定のアクセス装置識別情報と該データ記録装置の記憶領域に予め登録されている共通鍵および第１識別情報とにより暗号化された該コンテンツ鍵を書き込むステップと、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、該アクセス装置において、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報とにより、前記暗号化されたコンテンツ鍵を復号化するステップと、復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとを含むことを特徴とする、データ保護方法。

【０１０４】（付記３）　該データ記録装置の認証を行なうステップが、該データ記録装置の記憶領域に予め登録されている共通鍵および第１識別情報を該データ記録装置から該アクセス装置へ転送するステップと、該アクセス装置で乱数を発生するステップと、該乱数を該アクセス装置から該データ記録装置へ転送するステップと、該データ記録装置の記憶領域に予め登録されている第２識別情報を該データ記録装置から該アクセス装置へ転送するステップと、該データ記録装置において、該第２識別情報を、該アクセス装置からの前記乱数と該データ記録装置の秘密鍵とにより暗号化するステップと、暗号化された第２識別情報を該データ記録装置から該アクセス装置へ転送するステップと、該アクセス装置において、該第２識別情報を前記の乱数，共通鍵および第１識別情報により暗号化するステップと、該データ記録装置からの前記暗号化された第２識別情報と該アクセス装置で暗号化された第２識別情報とを比較し、一致するか否かを判断するステップとを含み、これらの第２識別情報が一致すると判断された場合、該データ記録装置が認証されることを特徴とする、付記１または付記２に記載のデータ保護方法。

【０１０５】（付記４）　データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するためのシステムであって、該データ記録装置が、共通鍵，第１識別情報および第２識別情報を保持する第１記憶領域と、該アクセス装置からの要求に応じて、前記の共通鍵，第１識別情報および第２識別情報のうちの少なくとも一つを該第１記憶領域から読み出して該アクセス装置へ転送する第１転送手段と、該アクセス装置からの要求に応じて、該第２識別情報を、当該要求とともに該アクセス装置から送られてくる乱数と該データ記録装置の秘密鍵とにより暗号化する第１暗号化手段と、該第１暗号化手段により暗号化された第２識別情報を該アクセス装置へ転送する第２転送手段と、該アクセス装置からのコンテンツデータおよびコンテンツ鍵を書き込まれて保存する保存部とをそなえて構成されるとともに、該アクセス装置が、当該アクセス装置のアクセス装置識別情報を保持する第２記憶領域と、前記乱数を発生する第１乱数発生手段と、該第１乱数発生手段で発生された該乱数を該データ記録装置へ転送する第４転送手段と、該データ記録装置の該第１記憶領域から読み出された該第２識別情報を、該第１乱数発生手段で発生された該乱数と、該データ記録装置の該第１記憶領域から読み出された前記の共通鍵および第１識別情報とにより暗号化する第２暗号化手段と、該データ記録装置からの前記暗号化された第２識別情報と該第２暗号化手段で暗号化された第２識別情報とを比較し、一致するか否かを判断する第１比較判断手段と、これらの第２識別情報が一致すると該第１比較判断手段が判断した場合、該第２記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第１識別情報とにより、コンテンツ鍵を暗号化する第３暗号化手段と、該第３暗号化手段により暗号化されたコンテンツ鍵を、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第５転送手段と、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化する第４暗号化手段と、該第４暗号化手段により暗号化されたコンテンツデータを、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第６転送手段とをそなえて構成されたことを特徴とする、データ保護システム。

【０１０６】（付記５）　データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するためのシステムであって、該データ記録装置が、共通鍵，第１識別情報および第２識別情報を保持する第１記憶領域と、該

アクセス装置からの要求に応じて、前記の共通鍵，第１識別情報および第２識別情報のうちの少なくとも一つを該第１記憶領域から読み出して該アクセス装置へ転送する第１転送手段と、該アクセス装置からの要求に応じて、該第２識別情報を、当該要求とともに該アクセス装置から送られてくる乱数と該データ記録装置の秘密鍵とにより暗号化する第１暗号化手段と、該第１暗号化手段により暗号化された第２識別情報を該アクセス装置へ転送する第２転送手段と、コンテンツ鍵により暗号化されたコンテンツデータと、所定のアクセス装置識別情報と前記の共通鍵および第１識別情報とにより暗号化された該コンテンツ鍵とを予め書き込まれて保存する保存部と、該アクセス装置からの要求に応じて、前記暗号化されたコンテンツデータおよび前記暗号化されたコンテンツ鍵を該保存部から読み出して該アクセス装置へ転送する第３転送手段とをそなえて構成されるとともに、該アクセス装置が、当該アクセス装置のアクセス装置識別情報を保持する第２記憶領域と、前記乱数を発生する第１乱数発生手段と、該第１乱数発生手段で発生された該乱数を該データ記録装置へ転送する第４転送手段と、該データ記録装置の該第１記憶領域から読み出された該第２識別情報を、該第１乱数発生手段で発生された該乱数と、該データ記録装置の該第１記憶領域から読み出された前記の共通鍵および第１識別情報とにより暗号化する第２暗号化手段と、該データ記録装置からの前記暗号化された第２識別情報と該第２暗号化手段で暗号化された第２識別情報とを比較し、一致するか否かを判断する第１比較判断手段と、これらの第２識別情報が一致すると該第１比較判断手段が判断した場合、該第２記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第１識別情報とにより、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツ鍵を復号化する第１復号化手段と、該第１復号化手段により復号化されたコンテンツ鍵により、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツデータを復号化する第２復号化手段とをそなえて構成されたことを特徴とする、データ保護システム。

【０１０７】（付記６） 共通鍵，第１識別情報および第２識別情報を保持する第１記憶領域と、外部からの要求に応じて前記の共通鍵，第１識別情報および第２識別情報のうちの少なくとも一つを該第１記憶領域から読み出して要求元へ転送する第１転送手段と、外部からの要求に応じて、該第２識別情報を、当該要求とともに送られてくる乱数と秘密鍵とにより暗号化する第１暗号化手段と、該第１暗号化手段により暗号化された第２識別情報を要求元へ転送する第２転送手段と、該アクセス装置からのコンテンツデータおよびコンテンツ鍵を書き込まれて保存する保存部とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置であって、当該アクセス装置のアクセス装置識別情報を保持する第２記憶領域と、前記乱数を発生する第１乱数発生手段と、該第１乱数発生手段で発生された該乱数を該データ記録装置へ転送する第４転送手段と、該データ記録装置の該第１記憶領域から読み出された該第２識別情報を、該第１乱数発生手段で発生された該乱数と、該データ記録装置の該第１記憶領域から読み出された前記の共通鍵および第１識別情報とにより暗号化する第２暗号化手段と、該データ記録装置からの前記暗号化された第２識別情報と該第２暗号化手段で暗号化された第２識別情報とを比較し、一致するか否かを判断する第１比較判断手段と、これらの第２識別情報が一致すると該第１比較判断手段が判断した場合、該第２記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第１識別情報とにより、コンテンツ鍵を暗号化する第３暗号化手段と、該第３暗号化手段により暗号化されたコンテンツ鍵を、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第５転送手段と、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化する第４暗号化手段と、該第４暗号化手段により暗号化されたコンテンツデータを、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第６転送手段とをそなえて構成されたことを特徴とする、アクセス装置。

【０１０８】（付記７） 共通鍵，第１識別情報および第２識別情報を保持する第１記憶領域と、外部からの要求に応じて前記の共通鍵，第１識別情報および第２識別情報のうちの少なくとも一つを該第１記憶領域から読み出して要求元へ転送する第１転送手段と、外部からの要求に応じて、該第２識別情報を、当該要求とともに送られてくる乱数と該データ記録装置の秘密鍵とにより暗号化する第１暗号化手段と、該第１暗号化手段により暗号化された第２識別情報を要求元へ転送する第２転送手段と、コンテンツ鍵により暗号化されたコンテンツデータを書き込まれて保存するとともに所定のアクセス装置識別情報と前記の共通鍵および第１識別情報とにより暗号化された該コンテンツ鍵を書き込まれて保存する保存部と、外部からの要求に応じて前記暗号化されたコンテンツデータおよび前記暗号化されたコンテンツ鍵を該保存部から読み出して要求元へ転送する第３転送手段とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置であって、当該アクセス装置のアクセス装置識別情報を保持する第２記憶領域と、前記乱数を発生する第１乱数発生手段と、該第１乱数発生手段で発生された該乱数を該データ記録装置へ転送する第４転送手段と、該データ記録装置の該第１記憶領域から読み出された該第２識別情報を、該第１乱数発生手段で発生された該乱数と、該データ記録装置の該第１記憶領域から読み出された前記の共通鍵および第１識別情報とにより暗号化する第２暗号化手段と、該データ記録装置からの前記暗号化された第２識別情報と該第２暗号化手段で暗号化され

た第２識別情報とを比較し、一致するか否かを判断する第１比較判断手段と、これらの第２識別情報が一致すると該第１比較判断手段が判断した場合、該第２記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第１識別情報とにより、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツ鍵を復号化する第１復号化手段と、該第１復号化手段により復号化されたコンテンツ鍵により、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツデータを復号化する第２復号化手段とをそなえて構成されたことを特徴とする、アクセス装置。

【０１０９】（付記８） 共通鍵，第１識別情報および第２識別情報を保持する第１記憶領域と、外部からの要求に応じて前記の共通鍵，第１識別情報および第２識別情報のうちの少なくとも一つを該第１記憶領域から読み出して要求元へ転送する第１転送手段と、外部からの要求に応じて、該第２識別情報を、当該要求とともに送られてくる乱数と秘密鍵とにより暗号化する第１暗号化手段と、該第１暗号化手段により暗号化された第２識別情報を要求元へ転送する第２転送手段と、コンテンツ鍵により暗号化されたコンテンツデータを書き込まれて保存するとともに所定のアクセス装置識別情報と前記の共通鍵および第１識別情報とにより暗号化された該コンテンツ鍵を書き込まれて保存する保存部と、外部からの要求に応じて前記暗号化されたコンテンツデータおよび前記暗号化されたコンテンツ鍵を該保存部から読み出して要求元へ転送する第３転送手段とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置であって、当該アクセス装置のアクセス装置識別情報を保持する記憶領域と、前記乱数を発生する第１乱数発生手段と、該第１乱数発生手段で発生された該乱数を該データ記録装置へ転送する第４転送手段と、該データ記録装置の該第１記憶領域から読み出された該第２識別情報を、該第１乱数発生手段で発生された該乱数と、該データ記録装置の該第１記憶領域から読み出された前記の共通鍵および第１識別情報とにより暗号化する第２暗号化手段と、該データ記録装置からの前記暗号化された第２識別情報と該第２暗号化手段で暗号化された第２識別情報とを比較し、一致するか否かを判断する第１比較判断手段と、これらの第２識別情報が一致すると該第１比較判断手段が判断した場合で且つコンテンツデータを該データ記録装置に記録・保存する場合、該第２記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第１識別情報とにより、コンテンツ鍵を暗号化する第３暗号化手段と、該第３暗号化手段により暗号化されたコンテンツ鍵を、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第５転送手段と、該データ記録装置に記録・保存すべき前記コンテンツデータを、該コンテンツ鍵により暗号化する第４暗号化手段と、該第４暗号化手段により暗号化されたコンテンツデータを、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第６転送手段と、前記の第２識別情報が一致すると該第１比較判断手段が判断した場合で且つ該データ記録装置からコンテンツデータを読み出す場合、該第２記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第１識別情報とにより、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツ鍵を復号化する第１復号化手段と、該第１復号化手段により復号化されたコンテンツ鍵により、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツデータを復号化する第２復号化手段とをそなえて構成されたことを特徴とする、アクセス装置。

【０１１０】（付記９） 共通鍵，第１識別情報および第２識別情報を保持する第１記憶領域と、外部からの要求に応じて前記の共通鍵，第１識別情報および第２識別情報のうちの少なくとも一つを該第１記憶領域から読み出して要求元へ転送する第１転送手段と、外部からの要求に応じて、該第２識別情報を、当該要求とともに送られてくる乱数と秘密鍵とにより暗号化する第１暗号化手段と、該第１暗号化手段により暗号化された第２識別情報を要求元へ転送する第２転送手段と、該アクセス装置からのコンテンツデータおよびコンテンツ鍵を書き込まれて保存する保存部とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置としてコンピュータを機能させるアクセスプログラムであって、前記乱数を発生する第１乱数発生手段、該第１乱数発生手段で発生された該乱数を該データ記録装置へ転送する第４転送手段、該データ記録装置の該第１記憶領域から読み出された該第２識別情報を、該第１乱数発生手段で発生された該乱数と、該データ記録装置の該第１記憶領域から読み出された前記の共通鍵および第１識別情報とにより暗号化する第２暗号化手段、該データ記録装置からの前記暗号化された第２識別情報と該第２暗号化手段で暗号化された第２識別情報とを比較し、一致するか否かを判断する第１比較判断手段、これらの第２識別情報が一致すると該第１比較判断手段が判断した場合、当該アクセス装置のアクセス装置識別情報と前記の共通鍵および第１識別情報とにより、コンテンツ鍵を暗号化する第３暗号化手段、該第３暗号化手段により暗号化されたコンテンツ鍵を、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第５転送手段、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化する第４暗号化手段、および、該第４暗号化手段により暗号化されたコンテンツデータを、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第６転送手段として、該コンピュータを機能させることを特徴とする、アクセスプログラム。

【０１１１】（付記１０） 共通鍵，第１識別情報およ

び第２識別情報を保持する第１記憶領域と、外部からの要求に応じて前記の共通鍵，第１識別情報および第２識別情報のうちの少なくとも一つを該第１記憶領域から読み出して要求元へ転送する第１転送手段と、外部からの要求に応じて、該第２識別情報を、当該要求とともに送られてくる乱数と該データ記録装置の秘密鍵とにより暗号化する第１暗号化手段と、該第１暗号化手段により暗号化された第２識別情報を要求元へ転送する第２転送手段と、コンテンツ鍵により暗号化されたコンテンツデータを書き込まれて保存するとともに所定のアクセス装置識別情報と前記の共通鍵および第１識別情報とにより暗号化された該コンテンツ鍵を書き込まれて保存する保存部と、外部からの要求に応じて前記暗号化されたコンテンツデータおよび前記暗号化されたコンテンツ鍵を該保存部から読み出して要求元へ転送する第３転送手段とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置としてコンピュータを機能させるアクセスプログラムであって、前記乱数を発生する第１乱数発生手段、該第１乱数発生手段で発生された該乱数を該データ記録装置へ転送する第４転送手段、該データ記録装置の該第１記憶領域から読み出された該第２識別情報を、該第１乱数発生手段で発生された該乱数と、該データ記録装置の該第１記憶領域から読み出された前記の共通鍵および第１識別情報とにより暗号化する第２暗号化手段、該データ記録装置からの前記暗号化された第２識別情報と該第２暗号化手段で暗号化された第２識別情報とを比較し、一致するか否かを判断する第１比較判断手段、これらの第２識別情報が一致すると該第１比較判断手段が判断した場合、当該アクセス装置のアクセス装置識別情報と前記の共通鍵および第１識別情報とにより、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツ鍵を復号化する第１復号化手段、および、該第１復号化手段により復号化されたコンテンツ鍵により、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツデータを復号化する第２復号化手段として、該コンピュータを機能させることを特徴とする、アクセスプログラム。

【０１１２】（付記１１）　共通鍵，第１識別情報および第２識別情報を保持する第１記憶領域と、外部からの要求に応じて前記の共通鍵，第１識別情報および第２識別情報のうちの少なくとも一つを該第１記憶領域から読み出して要求元へ転送する第１転送手段と、外部からの要求に応じて、該第２識別情報を、当該要求とともに送られてくる乱数と秘密鍵とにより暗号化する第１暗号化手段と、該第１暗号化手段により暗号化された第２識別情報を要求元へ転送する第２転送手段と、該アクセス装置からのコンテンツデータおよびコンテンツ鍵を書き込まれて保存する保存部とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置としてコンピュータを機能させるアクセスプログラムを記録したコンピュータ読取可能な記録媒体であって、該アクセスプログラムが、前記乱数を発生する第１乱数発生手段、該第１乱数発生手段で発生された該乱数を該データ記録装置へ転送する第４転送手段、該データ記録装置の該第１記憶領域から読み出された該第２識別情報を、該第１乱数発生手段で発生された該乱数と、該データ記録装置の該第１記憶領域から読み出された前記の共通鍵および第１識別情報とにより暗号化する第２暗号化手段、該データ記録装置からの前記暗号化された第２識別情報と該第２暗号化手段で暗号化された第２識別情報とを比較し、一致するか否かを判断する第１比較判断手段、これらの第２識別情報が一致すると該第１比較判断手段が判断した場合、当該アクセス装置のアクセス装置識別情報と前記の共通鍵および第１識別情報とにより、コンテンツ鍵を暗号化する第３暗号化手段、該第３暗号化手段により暗号化されたコンテンツ鍵を、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第５転送手段、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化する第４暗号化手段、および、該第４暗号化手段により暗号化されたコンテンツデータを、該データ記録装置の該保存部に書き込むべく、該データ記録装置へ転送する第６転送手段として、該コンピュータを機能させることを特徴とする、アクセスプログラムを記録したコンピュータ読取可能な記録媒体。

【０１１３】（付記１２）　共通鍵，第１識別情報および第２識別情報を保持する第１記憶領域と、外部からの要求に応じて前記の共通鍵，第１識別情報および第２識別情報のうちの少なくとも一つを該第１記憶領域から読み出して要求元へ転送する第１転送手段と、外部からの要求に応じて、該第２識別情報を、当該要求とともに送られてくる乱数と該データ記録装置の秘密鍵とにより暗号化する第１暗号化手段と、該第１暗号化手段により暗号化された第２識別情報を要求元へ転送する第２転送手段と、コンテンツ鍵により暗号化されたコンテンツデータを書き込まれて保存するとともに所定のアクセス装置識別情報と前記の共通鍵および第１識別情報とにより暗号化された該コンテンツ鍵を書き込まれて保存する保存部と、外部からの要求に応じて前記暗号化されたコンテンツデータおよび前記暗号化されたコンテンツ鍵を該保存部から読み出して要求元へ転送する第３転送手段とをそなえて構成されるデータ記録装置に、アクセスするアクセス装置としてコンピュータを機能させるアクセスプログラムを記録したコンピュータ読取可能な記録媒体であって、該アクセスプログラムが、前記乱数を発生する第１乱数発生手段、該第１乱数発生手段で発生された該乱数を該データ記録装置へ転送する第４転送手段、該データ記録装置の該第１記憶領域から読み出された該第２識別情報を、該第１乱数発生手段で発生された該乱数と、該データ記録装置の該第１記憶領域から読み出され

た前記の共通鍵および第１識別情報とにより暗号化する第２暗号化手段、該データ記録装置からの前記暗号化された第２識別情報と該第２暗号化手段で暗号化された第２識別情報とを比較し、一致するか否かを判断する第１比較判断手段、これらの第２識別情報が一致すると該第１比較判断手段が判断した場合、当該アクセス装置のアクセス装置識別情報と前記の共通鍵および第１識別情報とにより、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツ鍵を復号化する第１復号化手段、および、該第１復号化手段により復号化されたコンテンツ鍵により、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツデータを復号化する第２復号化手段として、該コンピュータを機能させることを特徴とする、アクセスプログラムを記録したコンピュータ読取可能な記録媒体。

【０１１４】（付記１３）　データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置が初期状態である時に該データ記録装置に最初に接続された該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報を、該アクセス装置から該データ記録装置へ転送し、１回のみ書込可能な記憶領域に書き込むステップと、以後、該アクセス装置が該データ記録装置にアクセスする都度、該データ記録装置において、前記１回のみ書込可能な記憶領域に書き込まれた該アクセス装置識別情報に基づき、該アクセス装置の認証を行なうステップと、該アクセス装置が認証された場合、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合で且つコンテンツデータを該データ記録装置に記録・保存する場合、該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報によりコンテンツ鍵を暗号化するステップと、暗号化されたコンテンツ鍵を、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップと、該アクセス装置において、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化するステップと、暗号化されたコンテンツデータを、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴とする、データ保護方法。

【０１１５】（付記１４）　該アクセス装置および該データ記録装置がいずれも認証された場合で且つ該データ記録装置からコンテンツデータを読み出す場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、該アクセス装置において、該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報により、前記暗号化されたコンテンツ鍵を復号化するステップと、復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとをさらに含むことを特徴とする、付記１３記載のデータ保護方法。

【０１１６】（付記１５）　データを記録・保存するデータ記録装置と、該データ記録装置にアクセスするアクセス装置との間でデータ転送を行なう際に、該データ記録装置のデータを不正なアクセスから保護するための方法であって、該データ記録装置が初期状態である時に該データ記録装置に最初に接続された該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報を、該アクセス装置から該データ記録装置へ転送し、１回のみ書込可能な記憶領域に書き込むステップと、以後、該アクセス装置が該データ記録装置にアクセスする都度、該データ記録装置において、前記１回のみ書込可能な記憶領域に書き込まれた該アクセス装置識別情報に基づき、該アクセス装置の認証を行なうステップと、該アクセス装置が認証された場合、該アクセス装置において該データ記録装置の認証を行なうステップと、該データ記録装置が認証された場合で且つコンテンツデータを該データ記録装置に記録・保存する場合、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報とにより、コンテンツ鍵を暗号化するステップと、暗号化されたコンテンツ鍵を、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップと、該アクセス装置において、該データ記録装置に記録・保存すべきコンテンツデータを、該コンテンツ鍵により暗号化するステップと、暗号化されたコンテンツデータを、該データ記録装置に書き込むべく、該アクセス装置から該データ記録装置へ転送するステップとを含むことを特徴とする、データ保護方法。

【０１１７】（付記１６）　該アクセス装置および該データ記録装置がいずれも認証された場合で且つ該データ記録装置からコンテンツデータを読み出す場合、該データ記録装置における前記暗号化されたコンテンツデータと前記暗号化されたコンテンツ鍵とを該データ記録装置から読み出して該アクセス装置へ転送するステップと、該アクセス装置において、該アクセス装置の記憶領域に予め登録されているアクセス装置識別情報と該データ記録装置の記憶領域から読み出された共通鍵および第１識別情報とにより、前記暗号化されたコンテンツ鍵を復号化するステップと、復号化されたコンテンツ鍵により前記暗号化されたコンテンツデータを復号化するステップとをさらに含むことを特徴とする、付記１５記載のデータ保護方法。

【０１１８】（付記１７）　該アクセス装置の認証を行なうステップが、該データ記録装置で乱数を発生するステップと、該乱数を該データ記録装置から該アクセス装

置へ転送するステップと、該データ記録装置において、該アクセス装置識別情報を前記乱数により暗号化するステップと、該アクセス装置において、該アクセス装置識別情報を該データ記録装置からの前記乱数により暗号化するステップと、暗号化された該アクセス装置識別情報を該アクセス装置から該データ記録装置へ転送するステップと、該アクセス装置からの前記暗号化されたアクセス装置識別情報と該データ記録装置で暗号化されたアクセス装置識別情報とを比較し、一致するか否かを判断するステップとを含み、これらのアクセス装置識別情報が一致すると判断された場合、該アクセス装置が認証されることを特徴とする、付記１３～付記１６のいずれか一つに記載のデータ保護方法。

【０１１９】（付記１８）　該データ記録装置の認証を行なうステップが、該データ記録装置の記憶領域に予め登録されている共通鍵および第１識別情報を該データ記録装置から該アクセス装置へ転送するステップと、該アクセス装置で乱数を発生するステップと、該乱数を該アクセス装置から該データ記録装置へ転送するステップと、該データ記録装置の記憶領域に予め登録されている第２識別情報を該データ記録装置から該アクセス装置へ転送するステップと、該データ記録装置において、該第２識別情報を、該アクセス装置からの前記乱数と該データ記録装置の秘密鍵とにより暗号化するステップと、暗号化された第２識別情報を該データ記録装置から該アクセス装置へ転送するステップと、該アクセス装置において、該第２識別情報を前記の乱数，共通鍵および第１識別情報により暗号化するステップと、該データ記録装置からの前記暗号化された第２識別情報と該アクセス装置で暗号化された第２識別情報とを比較し、一致するか否かを判断するステップとを含み、これらの第２識別情報が一致すると判断された場合、該データ記録装置が認証されることを特徴とする、付記１３～付記１７のいずれか一つに記載のデータ保護方法。

【０１２０】（付記１９）　該データ記録装置が、初期状態の時に最初に接続された該アクセス装置のアクセス装置識別情報を書き込まれる、１回のみ書込可能な記憶領域と、該アクセス装置からアクセスされる都度、該データ記録装置で乱数を発生する第２乱数発生手段と、該第２乱数発生手段で発生された該乱数を該アクセス装置へ転送する第７転送手段と、前記１回のみ書込可能な記憶領域から読み出された該アクセス装置識別情報を、該第２乱数発生手段で発生された該乱数により暗号化する第５暗号化手段と、該第５暗号化手段で暗号化されたアクセス装置識別情報と、該アクセス装置からの、該乱数により暗号化されたアクセス装置識別情報とを比較し、一致するか否かを判断する第２比較判断手段とをさらにそなえるとともに、該アクセス装置が、初期状態の該データ記録装置に最初に接続された時に、該アクセス装置識別情報を該第２記憶領域から読み出して該データ記録装置へ転送する第８転送手段と、該アクセス装置識別情報を、該データ記録装置から送られてくる乱数により暗号化する第６暗号化手段と、該データ記録装置にアクセスする都度、該第６暗号化手段により暗号化されたアクセス装置識別情報を該データ記録装置へ転送する第９転送手段とをさらにそなえ、該第１比較判断手段および該第２比較判断手段がいずれも識別情報が一致すると判断した場合で且つコンテンツデータを該データ記録装置に記録・保存する場合に、該第３暗号化手段，該第５転送手段，該第４暗号化手段および該第６転送手段が動作することを特徴とする、付記４記載のデータ保護システム。

【０１２１】（付記２０）　該データ記録装置が、該アクセス装置からの要求に応じて、前記暗号化されたコンテンツデータおよび前記暗号化されたコンテンツ鍵を該保存部から読み出して該アクセス装置へ転送する第３転送手段をさらにそなえて構成されるとともに、該アクセス装置が、該第１比較判断手段および該第２比較判断手段がいずれも識別情報が一致すると判断した場合で且つ該データ記録装置からコンテンツデータを読み出す場合、該第２記憶領域から読み出された該アクセス装置識別情報と、前記の共通鍵および第１識別情報とにより、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツ鍵を復号化する第１復号化手段と、該第１復号化手段により復号化されたコンテンツ鍵により、該データ記録装置の該保存部から読み出された前記暗号化されたコンテンツデータを復号化する第２復号化手段とをそなえて構成されたことを特徴とする、付記１９記載のデータ保護システム。

【０１２２】（付記２１）　データを記録・保存し、アクセス装置からのアクセスに応じて該データの書込／読出を行なうデータ記録装置であって、初期状態の時に最初に接続された該アクセス装置のアクセス装置識別情報を書き込まれる、１回のみ書込可能な記憶領域と、該アクセス装置からアクセスされる都度、該データ記録装置で乱数を発生する第２乱数発生手段と、該第２乱数発生手段で発生された該乱数を該アクセス装置へ転送する第７転送手段と、前記１回のみ書込可能な記憶領域から読み出された該アクセス装置識別情報を、該第２乱数発生手段で発生された該乱数により暗号化する第５暗号化手段と、該第５暗号化手段で暗号化されたアクセス装置識別情報と、該アクセス装置からの、該乱数により暗号化されたアクセス装置識別情報とを比較し、一致するか否かを判断する第２比較判断手段とをそなえて構成されたことを特徴とする、データ記録装置。

【０１２３】

【発明の効果】以上詳述したように、本発明のデータ保護方法（請求項１，２）によれば、アクセス装置（ホスト）がコンテンツデータおよびコンテンツ鍵をデータ記録装置に書き込む際に、コンテンツ鍵が、データ記録装

置の識別情報にアクセス装置識別情報（ホストＩＤ）の要素を加えて暗号化されているので、コンテンツデータやコンテンツ鍵をデータ記録装置に書き込んだ正規のアクセス装置しか、そのコンテンツデータを読み出すことができない。つまり、正規のアクセス装置以外のアクセス装置がデータ記録装置からコンテンツデータを読み出しても、そのアクセス装置の識別情報が正規のものと異なっているため、コンテンツ鍵を正しく復号化することができないので、コンテンツデータを正しく復号化できず、コンテンツデータを読み出すことができなくなる。従って、ＣＰＰＭやＣＰＲＭ等の単方向認証を採用してデータ記録装置側での処理の負荷を大きくすることなく、データ記録装置のデータを不正なアクセスから保護することができ、データ記録装置側での不正コピーのみならず、アクセス装置側での成りすまし等によるデータの不正読出しや不正コピーをも確実に防止し、著作権を確実に保護することができる。

【０１２４】また、本発明のデータ保護方法（請求項３～５）によれば、データ記録装置（ドライブ）が初期状態である時にこのデータ記録装置に最初に接続されたアクセス装置（ホスト）の識別情報（ホストＩＤ）が、データ記録装置における１回のみ書込可能な記憶領域に書き込まれ、それ以降、その記憶領域に書き込まれた識別情報に基づいて、データ記録装置にアクセスしたアクセス装置が、当該データ記録装置に最初に接続されたアクセス装置（正規のアクセス装置）であるかどうかの認証が行なわれる。そして、正規のアクセス装置であると認証された場合のみ、データ記録装置に対するアクセス（データ書込／読出）が許可される。

【０１２５】これにより、データ記録装置側で極めて簡素な認証処理を行なうだけで、正規のアクセス装置以外のアクセス装置はデータ記録装置にアクセスすることができなくなる。従って、データ記録装置側での処理の負荷を大きくすることなく、データ記録装置のデータを不正なアクセスから保護することができ、データ記録装置側での不正コピーのみならず、アクセス装置側での成りすまし等によるデータの不正読出しや不正コピーをも確実に防止し、著作権を確実に保護することができる。

【０１２６】さらに、データ記録装置に最初に接続された正規のアクセス装置しかデータ記録装置にアクセスすることができなくなるので、例えばセットトップボックスからハードディスクドライブ（データ記録装置）を取り外しセットトップボックス以外のシステムで転用するといった、データ記録装置の不正転用をも確実に防止することができる。

【０１２７】なお、最初に接続されたアクセス装置の識別情報をデータ記録装置における１回のみ書込可能な記憶領域に書き込みその識別情報を用いてアクセス装置の認証を行なう技術と、データ記録装置に書き込むべきコンテンツ鍵をデータ記録装置識別情報およびアクセス装置識別情報により暗号化する技術とを組み合わせることにより、例え何らかの手段を用いてアクセス装置の認証を不正にくぐり抜けたとしても、正規のアクセス装置以外のアクセス装置では、データ記録装置から読み出されたコンテンツ鍵を復号化することができず、コンテンツデータを読み出せない。従って、アクセス装置側での成りすまし等によるデータの不正読出しや不正コピーをより確実に防止することができる。

【図面の簡単な説明】

【図１】本発明の第１実施形態としてのデータ保護方法を適用されたデータ保護システム（アクセス装置およびデータ記録装置）の機能構成を示すブロック図である。

【図２】第１実施形態のデータ保護システムにおけるコンテンツデータ書込動作に係る要部を取り出して示すブロック図である。

【図３】第１実施形態におけるコンテンツデータ書込手順を説明するための図である。

【図４】第１実施形態のデータ保護システムにおけるコンテンツデータ読出動作に係る要部を取り出して示すブロック図である。

【図５】第１実施形態におけるコンテンツデータ読出手順を説明するための図である。

【図６】本発明の第２実施形態としてのデータ保護方法を適用されたデータ保護システム（アクセス装置およびデータ記録装置）の機能構成を示すブロック図である。

【図７】第２実施形態のデータ保護システムにおけるコンテンツデータ書込動作に係る要部を取り出して示すブロック図である。

【図８】第２実施形態におけるコンテンツデータ書込手順を説明するための図である。

【図９】第２実施形態のデータ保護システムにおけるコンテンツデータ読出動作に係る要部を取り出して示すブロック図である。

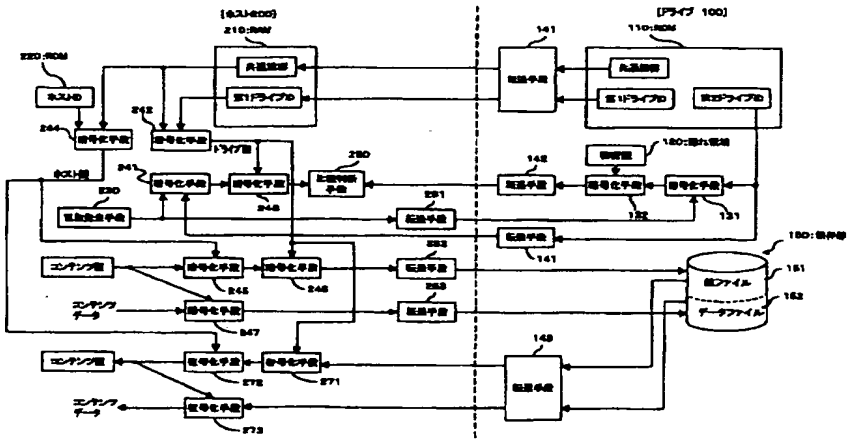
【図１０】第２実施形態におけるコンテンツデータ読出手順を説明するための図である。

【符号の説明】

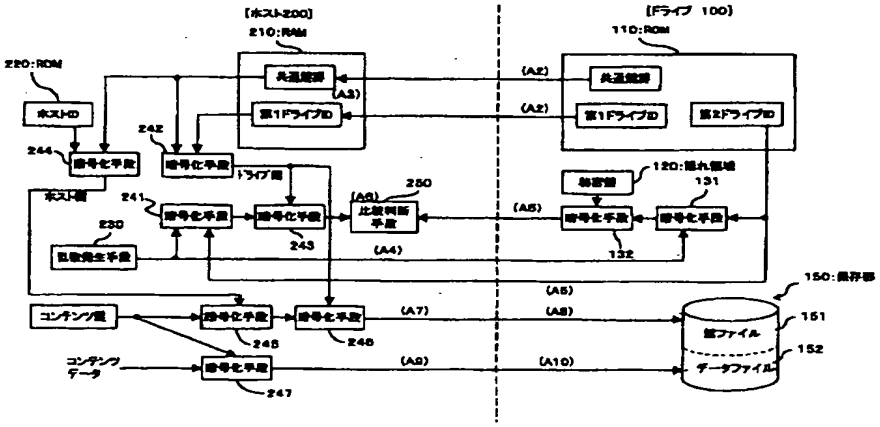
１００，１００Ａ　ドライブ（データ記録装置）
１１０　ＲＯＭ（第１記憶領域）
１２０　隠れ領域
１３１，１３２　暗号化手段（第１暗号化手段）
１３３　暗号化手段（第５暗号化手段）
１４１　転送手段（第１転送手段）
１４２　転送手段（第２転送手段）
１４３　転送手段（第３転送手段）
１４４　転送手段（第７転送手段）
１５０　保存部
１５１　鍵ファイル
１５２　データファイル
１６０　１回書込可能記憶領域
１７０　乱数発生手段（第２乱数発生手段）

１８０　比較判断手段（第２比較判断手段）
２００，２００Ａ　ホスト（アクセス装置）
２１０　ＲＡＭ
２２０　ＲＯＭ（第２記憶領域）
２３０　乱数発生手段（第１乱数発生手段）
２４１，２４３　暗号化手段（第２暗号化手段）
２４２　暗号化手段（第２暗号化手段，第３暗号化手段）
２４４，２４５，２４６　暗号化手段（第３暗号化手段）
２４７　暗号化手段（第４暗号化手段）
２４８　暗号化手段（第６暗号化手段）
２５０　比較判断手段（第１比較判断手段）
２６１　転送手段（第４転送手段）
２６２　転送手段（第５転送手段）
２６３　転送手段（第６転送手段）
２６４　転送手段（第８転送手段）
２６５　転送手段（第９転送手段）
２７１，２７２　復号化手段（第１復号化手段）
２７３　復号化手段（第２復号化手段）

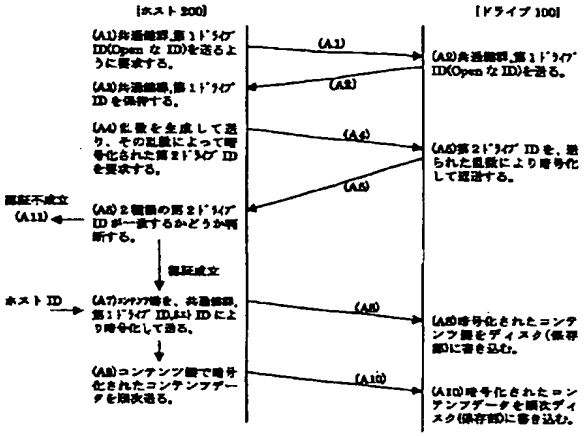
【図１】



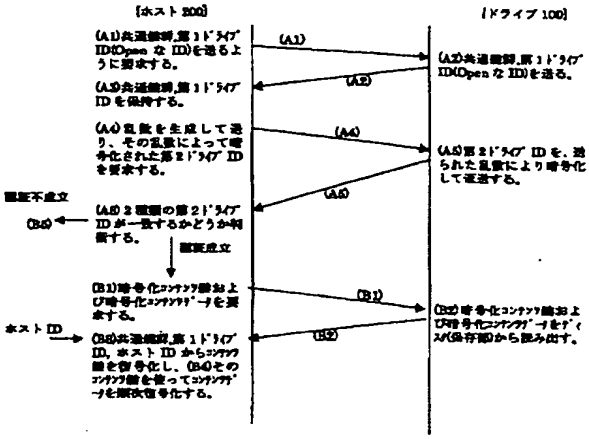
【図２】



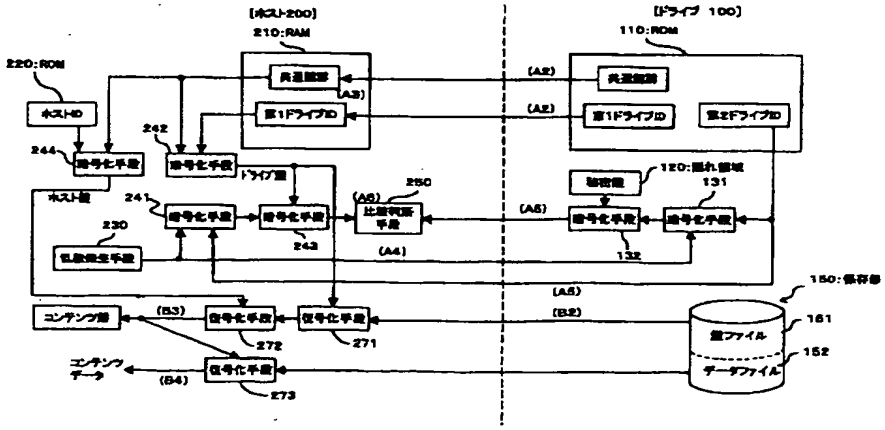
【図３】


[ホスト200]
[ドライブ100]
(A1)共通鍵暗号,第1ドライブID(Open なID)を送るように要求する。
(A1)
(A2)共通鍵暗号,第1ドライブID(Open なID)を送る。
(A2)
(A3)共通鍵暗号,第1ドライブIDを保持する。
(A4)乱数を生成して送り、その乱数によって暗号化された第2ドライブIDを要求する。
(A4)
(A5)第2ドライブIDを、送られた乱数により暗号化して返送する。
(A5)
認証不成立
(A11)
(A6)2個目の第2ドライブIDが一致するかどうか判断する。
認証成立
ホストID
(A7)コンテンツ鍵を、共通鍵暗号,第1ドライブID,ホストIDにより暗号化して送る。
(A8)
(A8)暗号化されたコンテンツ鍵をディスク(保存部)に書き込む。
(A9)コンテンツ鍵で暗号化されたコンテンツデータを順次送る。
(A10)
(A10)暗号化されたコンテンツデータを順次ディスク(保存部)に書き込む。

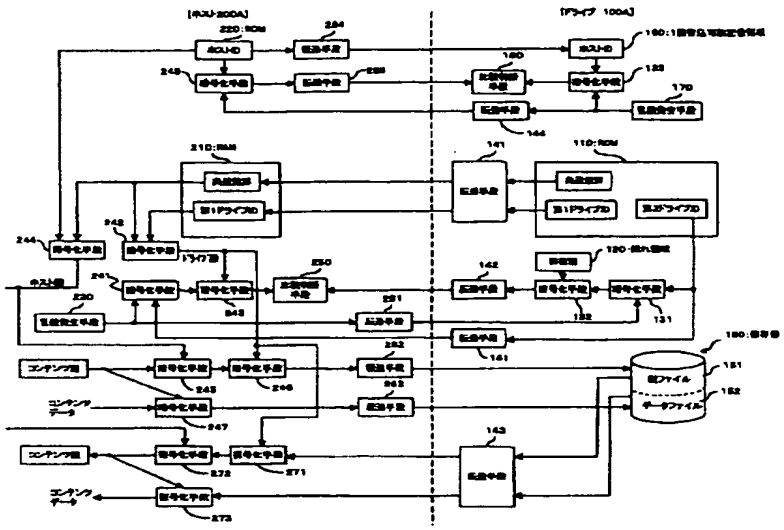
【図５】


[ホスト200]
[ドライブ100]
(A1)共通鍵暗号,第1ドライブID(Open なID)を送るように要求する。
(A1)
(A2)共通鍵暗号,第1ドライブID(Open なID)を送る。
(A2)
(A3)共通鍵暗号,第1ドライブIDを保持する。
(A4)乱数を生成して送り、その乱数によって暗号化された第2ドライブIDを要求する。
(A4)
(A5)第2ドライブIDを、送られた乱数により暗号化して返送する。
(A5)
認証不成立
(B6)
(A6)2個目の第2ドライブIDが一致するかどうか判断する。
認証成立
(B1)暗号化コンテンツ鍵およびコンテンツデータを要求する。
(B1)
(B2)暗号化コンテンツ鍵およびコンテンツデータを(保存部)から読み出す。
ホストID
(B5)共通鍵暗号,第1ドライブID,ホストIDからコンテンツ鍵を復号化し、(B4)そのコンテンツ鍵を使ってコンテンツデータを順次復号化する。
(B2)

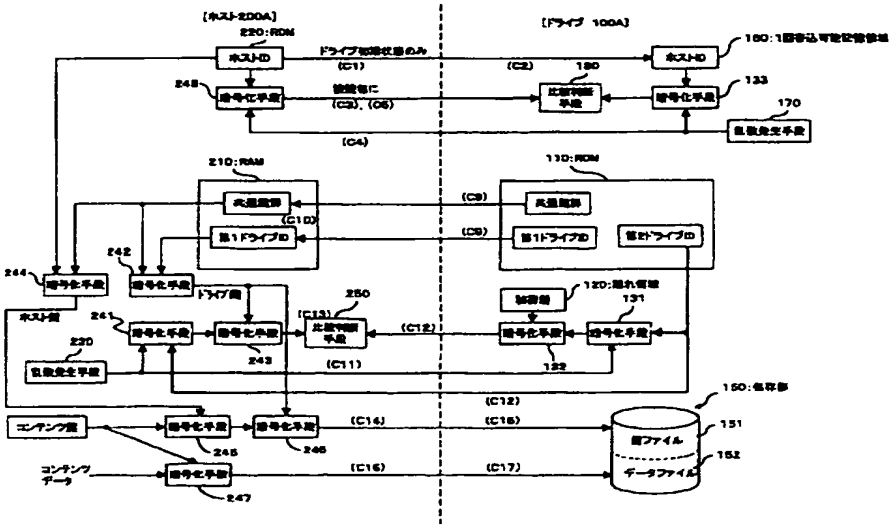
【図４】


[ホスト200]
210:RAM
[ドライブ 100]
110:ROM
220:ROM
共通鍵部
(A3)
第1ドライブID
(A2)
(A2)
共通鍵部
第1ドライブID
第2ドライブID
ホストID
242
244
暗号化手段
暗号化手段
ドライブ鍵
ホスト鍵
241
暗号化手段
暗号化手段
(A6)
250
比較判断手段
243
(A4)
230
乱数発生手段
(A5)
150:保存部
(B3)
コンテンツ鍵
暗号化手段
復号化手段
(B2)
161
鍵ファイル
272
271
152
データファイル
コンテンツデータ
(B4)
復号化手段
273

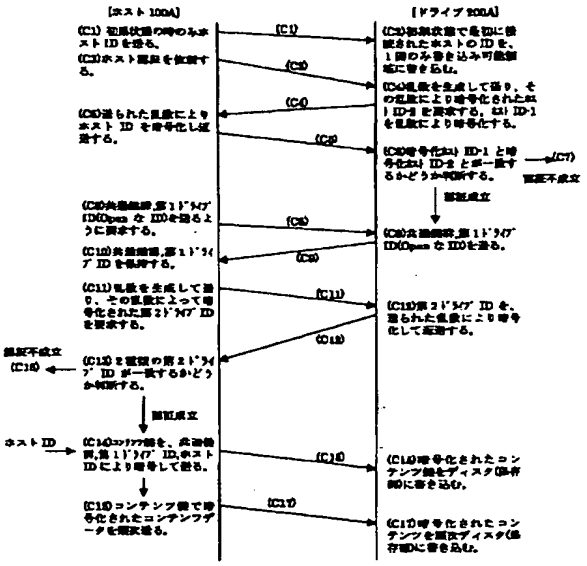
【図６】



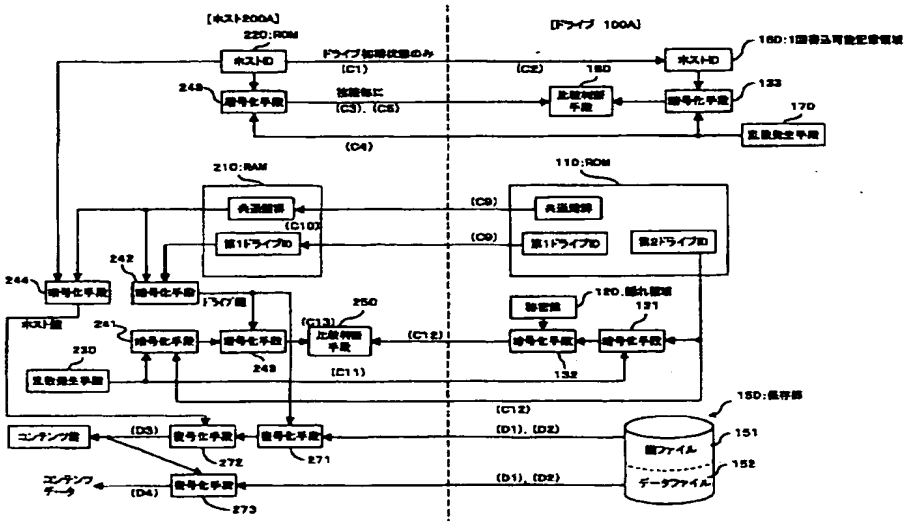
【図７】



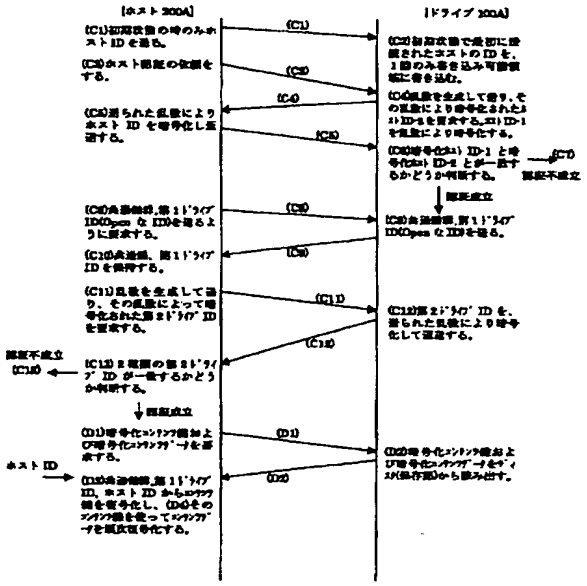
【図８】



【図９】



【図１０】



フロントページの続き

Ｆターム(参考) 5B017 AA06 AA07 BA07 BA09 CA15
5B065 BA01 CA17 CC08 CS06 PA04
PA16
5J104 AA01 AA07 AA16 EA04 EA17
JA03 NA02 PA14